ZATWIERDZAM

Jakub Zawierucha

Dyrektor

Dział Systemów Informatycznych

Warszawa, 23 kwietnia 2020 r.

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

(SIWZ)

Przedmiotem zamówienia jest dostawa licencji na system ochrony infrastruktury IT dla NCBR.
Postępowanie znak 18/20/PN/P24

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

1. ADRES ZAMAWIAJĄCEGO

adres: **NARODOWE CENTRUM BADAŃ I ROZWOJU w WARSZAWIE** ul. Nowogrodzka 47a 00-695 Warszawa **www.ncbr.gov.pl**	**Osoba upoważniona do kontaktów:** **Marzena Marczak** **przetargi@ncbr.gov.pl**

2. TRYB UDZIELENIA ZAMÓWIENIA

2.1. Niniejsze postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie art. 39 i nast. ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2019 r. poz. 1843 z póź. zm.) zwanej dalej „ustawą PZP" lub „uPzp" – oraz przepisów wykonawczych wydanych na jej podstawie, w szczególności rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016 r. *w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia* (Dz. U. z 2016 r. poz. 1126) – zwanego dalej „rozporządzeniem MR" – w trybie przetargu nieograniczonego.

2.2. W zakresie nieuregulowanym niniejszą Specyfikacją Istotnych Warunków Zamówienia, zwaną dalej „SIWZ", zastosowanie mają przepisy ustawy PZP.

2.3. Wartość niniejszego zamówienia jest niższa niż równowartość kwoty określonej w przepisach wykonawczych wydanych na podstawie art. 11 ust. 8 oraz art. 6a ustawy PZP.

2.4. Zgodnie z art. 24aa ustawy PZP, Zamawiający najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

3. OPIS PRZEDMIOTU ZAMÓWIENIA.

3.1. Pozycja we Wspólnym Słowniku **Zamówień CPV**:

48731000-1 - Pakiety oprogramowania zabezpieczającego pliki;

48000000-8 - Pakiety oprogramowania i systemy informatyczne;

48700000-5 - Pakiety oprogramowania użytkowego;

48730000-4 - Pakiety oprogramowania zabezpieczającego;

48732000-8 - Pakiety oprogramowania do zabezpieczania danych;

48760000-3 - Pakiety oprogramowania do ochrony antywirusowej.

3.2. Zamawiający informuje, że jest w posiadaniu licencji ważnych do dnia 2019-12-14:

3.2.1. **McAfee Complete Data Protection Advanced – 600 szt.**

3.2.2. **McAfee Threat Intelligence Exchange - 600 szt.**

3.2.3. **McAfee Complete EndPoint Threat Protection Enterprise - 600 szt.**

3.2.4. **McAfee Virtual Advanced Threat Defence Appliance - 1 szt.**

3.3. Zamawiający informuje, że jest w posiadaniu licencji do dnia 2020-05-25:

3.3.1. **McAfee Complete Data Protection Advanced – 100 szt.**

3.3.2. **McAfee Threat Intelligence Exchange - 100 szt.**

3.3.3. **McAfee Complete EndPoint Threat Protection Enterprise - 100 szt.**

3.4. Przedmiotem zamówienia jest:

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

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

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

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

3.4.4. odnowienia licencji pakietu McAfee Virtual Advanced Threat Defence Appliance – w ilości 1 (jednej) szt. ważnej od dnia 2019-12-15 do dnia 2021-05-25 roku;

3.4.5. odnowienia licencji pakietu McAfee Complete Data Protection Advanced – w ilości 100 (stu) szt. ważnej od dnia 2020-05-26 do dnia 2021-05-25 roku;

3.4.6. odnowienia licencji pakietu McAfee Threat Intelligence Exchange - w ilości 100 (stu) szt. ważnej od dnia 2020-05-26 do dnia 2021-05-25 roku

3.4.7. odnowienia licencji pakietu McAfee Complete EndPoint Threat Protection Enterprise – w ilości 100 (stu) szt. ważnej od dnia 2020-05-26 do dnia 2021-05-25 roku;

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

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

3.4.10. nowe licencje pakietu 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:

- 3.4.1 z 3.4.5 oraz 3.4.8
- 3.4.2 z 3.4.6 oraz 3.4.9
- 3.4.3 z 3.4.7 oraz 3.4.10

3.5. Szczegółowy opis przedmiotu zamówienia (SOPZ) znajduje się w Załączniku nr 1 do niniejszej Specyfikacji Istotnych Warunków Zamówienia (SIWZ) i stanowi jej integralną część.

3.6. Zamawiający nie przewiduje aukcji elektronicznej.

3.7. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

3.8. Zamawiający nie przewiduje: zawarcia umowy ramowej, zwrotu kosztów udziału w postępowaniu.

3.9. Zamawiający nie przewiduje ustanowienia dynamicznego systemu zakupów.

3.10. Zamawiający zastrzega obowiązek osobistego wykonania przez Wykonawcę kluczowych części zamówienia.

3.11. W przypadku rozbieżności pomiędzy treścią niniejszej SIWZ a treścią udzielonych wyjaśnień, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.

3.12. 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.

4. TERMIN WYKONANIA ZAMÓWIENIA

Termin wykonania zamówienia – do 7 (siedmiu) dni kalendarzowych od dnia podpisania umowy.

5. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIENIA TYCH WARUNKÓW

5.1. Udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy zgodnie z art 22 ust. 1:

5.1.1. nie podlegają wykluczeniu:

5.1.2. spełniają warunki udziału w postępowaniu, określone przez Zamawiającego w ogłoszeniu o zamówieniu i niniejszym SIWZ.

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

5.2.1. kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej,

5.2.2. zdolności technicznej lub zawodowej.

5.3. W zakresie warunku określonego w art. 22 ust. 1b pkt 3) ustawy PZP (zdolności technicznej lub zawodowej), Wykonawcy winni wykazać się:

5.3.1. warunku udziału w postępowaniu określonego w art. 22 ust. 1b pkt 3 ustawy PZP (zdolności technicznej lub zawodowej): Wykonawcy winni wykazać, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wykonał należycie, a w przypadku świadczeń okresowych lub ciągłych wykonuje należycie co najmniej dwie dostawy licencji na oprogramowanie ochrony infrastruktury IT o wartości każdej z nich co najmniej 50 000,00 zł (słownie: pięćdziesiąt tysięcy złotych) brutto;

Uwaga:

Zamawiający nie dopuszcza sumowania usług z różnych kontraktów w celu uzyskania wartości minimalnej.

Wykonawcy w celu wykazania spełnienia ww. warunków winni wykazać się realizacją minimum dwóch usług dla dwóch podmiotów.

W przypadku oferty składanej przez Wykonawców ubiegających się wspólnie o wykonanie zamówienia wystarczy, że warunek określony w pkt 5.3.1. SIWZ spełni jeden z nich lub Wykonawcy spełnią go łącznie.

Ocena spełnienia ww. warunku odbywać się będzie metodą spełnia/nie spełnia.

Do wykorzystania **Wykaz usług**, który stanowi Załącznik nr 5 do SIWZ.

5.4. Ocena spełnienia ww. warunku odbywać się będzie metodą spełnia/nie spełnia. Z treści załączonych dokumentów i oświadczeń musi wynikać jednoznacznie, iż Wykonawca spełnia wyżej wymienione warunki.

5.5. Niespełnienie chociażby jednego z warunków wymienionych w pkt 5.1 oraz 5.3 niniejszego SIWZ skutkować będzie wykluczeniem Wykonawcy z postępowania.

5.6. Zamawiający może, na każdym etapie postępowania, uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli zaangażowanie zasobów technicznych lub zawodowych Wykonawcy w inne przedsięwzięcia gospodarcze Wykonawcy może mieć negatywny wpływ na realizację zamówienia.

5.7. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, o których mowa w 5.3.1. SIWZ polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych. W takim przypadku:

5.7.1. Wykonawca, który polega na zdolnościach innych podmiotów musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

5.7.2. Zamawiający oceni, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 13–23 i ust. 5 ustawy PZP.

5.7.3. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują usługi, do realizacji których te zdolności są wymagane.

6. PODSTAWY WYKLUCZENIA, O KTÓRYCH MOWA W ART. 24 UST. 5 USTAWY PZP.

Zamawiający z przedmiotowego postępowania wykluczy Wykonawcę na podstawie art. 24 ust. 5 pkt 1 ustawy PZP tj. w stosunku, do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz.U. 2017 poz. 2344 ze zm.) lub którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz.U. 2017 poz. 2344 ze zm.).

7. INFORMACJE O OŚWIADCZENIACH I DOKUMENTACH, JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW DO WYKLUCZENIA

7.1. W celu potwierdzenia spełniania warunków udziału w postępowaniu oraz wykazania braku podstaw wykluczenia, określonych w pkt 5, Wykonawcy ubiegający się o udzielenie zamówienia muszą wraz z ofertą złożyć następujące dokumenty:

7.1.1. aktualne na dzień składania ofert oświadczenie w zakresie wskazanym odpowiednio w **Załączniku nr 3 do SIWZ**. Informacje zawarte w oświadczeniu będą stanowić wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

7.1.2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenie, o którym mowa w pkt 7.1.1. SIWZ **składa każdy z Wykonawców wspólnie ubiegających się o zamówienie**. Oświadczenie to potwierdza spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

7.1.3. W przypadku, kiedy Wykonawca zamierza powierzyć wykonanie części zamówienia podwykonawcy, Zamawiający żąda wskazania przez Wykonawcę w Formularzu oferty, części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, i podania przez Wykonawcę firm podwykonawców.

7.1.4. W przypadku, gdy Wykonawcy będą polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów. W tym celu, dodatkowo winni oni przedłożyć:

7.1.4.1. dokument potwierdzający, że będą dysponować zasobami innego podmiotu niezbędnymi do realizacji zamówienia np. pisemne zobowiązanie tego podmiotu do oddania do dyspozycji Wykonawcy niezbędnych zasobów na potrzeby realizacji zamówienia,

7.1.4.2. dokument (np. umowa Wykonawcy z podmiotem), określający w szczególności:

a) zakres dostępnych Wykonawcy zasobów innego podmiotu,

b) sposobu wykorzystania zasobów innego podmiotu, przez Wykonawcę, przy wykonywaniu zamówienia publicznego,

c) zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego.

Ww. dokument wymagany jest w celu oceny, czy Wykonawca będzie dysponował niezbędnymi zasobami innych podmiotów w stopniu umożliwiającym należyte wykonanie zamówienia publicznego oraz oceny, czy stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów. Dokument określony w pkt 7.1.4.2. SIWZ nie jest wymagany, o ile dokument określony w pkt 7.1.4.1. SIWZ będzie potwierdzał, że Wykonawca będzie dysponował zasobami innych podmiotów w stopniu umożliwiającym należyte wykonanie zamówienia oraz że stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, a jego treść będzie zawierała informacje, o których mowa w pkt 7.1.4.2. a)-c) SIWZ.

7.1.5. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełnienia – w zakresie, w jakim powołuje się na ich zasoby – warunków udziału w postępowaniu, zamieszcza w oświadczeniu, o którym mowa w pkt 7.1.1., informacje o tych podmiotach.

7.2. Zamawiający przed udzieleniem zamówienia, wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni terminie:

7.2.1. **aktualnego**[1] na dzień złożenia **odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej**, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw do wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy PZP.

7.2.2. **oświadczenia Wykonawcy** o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo – w przypadku wydania takiego wyroku lub decyzji - dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności. Oświadczenie należy sporządzić zgodnie z Załącznikiem nr 3 do SIWZ;

7.2.3. **oświadczenia Wykonawcy** o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne. Oświadczenie należy sporządzić zgodnie z Załącznikiem nr 3 do SIWZ;

7.2.4. **Wykazu usług** z podaniem przedmiotu usługi, wartości, dat wykonania, nazwy podmiotu na rzecz, którego była świadczona dostawa **oraz załączenie dowodów w rozumieniu Rozporządzenia**, że zostały wykonane należycie. Do ewentualnego wykorzystania przy sporządzaniu tego dokumentu służy Załącznik nr 5 do SIWZ.

Uwaga:

W przypadku Wykonawców:

a) wspólnie ubiegających się o zamówienie, dokument wymieniony w pkt 7.2.1. powyżej, składa każdy z Wykonawców występujących wspólnie;

b) polegających na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy, dokument wymieniony w pkt 7.2. powyżej, Wykonawca składa w odniesieniu do każdego z tych podmiotów;

7.3. Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy PZP, przekaże Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy PZP. Do sporządzania oświadczenia służy Załącznik nr 4 do SIWZ. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

[1] Za aktualny uważa się dokument, w którym, w zakresie objętych nim faktów, utrzymują się okoliczności nim potwierdzone, ważny na dzień wyznaczony, jako termin składania ofert.

7.4. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentu, o którym mowa w pkt 7.2. powyżej składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające, że nie otwarto jego likwidacji ani nie ogłoszono upadłości, wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

7.5. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w pkt 7.4. powyżej, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy lub miejsce zamieszkania tej osoby. Dokumenty muszą być wystawione w terminach analogicznych jak wskazane w pkt 7.4. powyżej.

W przypadku wątpliwości co do treści dokumentu złożonego przez Wykonawcę, Zamawiający może zwrócić się do właściwych organów kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.

7.6. W przypadku wątpliwości co do treści dokumentu złożonego przez Wykonawcę, Zamawiający może zwrócić się do właściwych organów kraju, w którym miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu. W przypadku wskazania przez Wykonawcę dostępności oświadczeń lub dokumentów wymienionych w pkt 7.2. powyżej, w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający pobiera samodzielnie z tych baz danych wskazane przez Wykonawcę oświadczenia lub dokumenty.

7.7. W przypadku wskazania przez Wykonawcę oświadczeń lub dokumentów, o których mowa powyżej, które znajdują się w posiadaniu Zamawiającego, w szczególności oświadczeń lub dokumentów przechowywanych przez Zamawiającego zgodnie z art. 97 ust. 1 ustawy PZP, Zamawiający w celu potwierdzenia okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3 usta0wy, korzysta z posiadanych oświadczeń lub dokumentów, o ile są one aktualne.

7.8. W przypadku wskazania przez Wykonawcę dostępności oświadczeń lub dokumentów, o których mowa w pkt 7.2. powyżej, w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych Zamawiający pobiera samodzielnie z tych baz danych wskazane przez Wykonawcę oświadczenia lub dokumenty.

7.9. Jeżeli Wykonawca nie złoży oświadczenia, o którym mowa w pkt 7.1.1. SIWZ, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy PZP, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wezwie do ich złożenia, uzupełnienia, poprawienia lub udzielenia wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlegała odrzuceniu albo konieczne byłoby unieważnienie postępowania. Jeżeli Wykonawca nie złożył wymaganych pełnomocnictw albo złożył wadliwe pełnomocnictwa,

Zamawiający wezwie do ich złożenia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.

7.10. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania wezwać Wykonawców do złożenia wszystkich lub niektórych oświadczeń lub dokumentów potwierdzających, że nie podlegają wykluczeniu, spełniają warunki udziału w postępowaniu, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio oświadczenia lub dokumenty nie są aktualne, do złożenia aktualnych oświadczeń lub dokumentów.

7.11. W przypadku podpisywania oferty przez pełnomocnika **wraz z ofertą Wykonawca winien złożyć oryginał pełnomocnictwa albo kopię** uwierzytelnioną notarialnie. Z treści pełnomocnictwa winno wynikać uprawnienie pełnomocnika do reprezentowania Wykonawcy.

7.12. **Wykonawcy ubiegający się wspólnie o udzielenie zamówienia** (np. spółki cywilne, konsorcja), zgodnie z art. 23 ust. 2 ustawy PZP, **zobowiązani są ustanowić pełnomocnika.** Z treści pełnomocnictwa winno jednoznacznie wynikać prawo pełnomocnika do reprezentowania Wykonawcy w postępowaniu o udzielenie zamówienia publicznego albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego w imieniu Wykonawcy. Dokument ten winien być podpisany przez osobę/osoby uprawnioną(-e) do jego udzielenia tj. zgodnie z formą reprezentacji każdego z Wykonawców. W przypadku wspólników spółki cywilnej dopuszczalne jest przedłożenie umowy spółki cywilnej, z której wynika zakres i sposób reprezentacji, a w przypadku konsorcjum przedłożenie umowy konsorcjum.

8. INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI

8.1. W niniejszym postępowaniu wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują pisemnie lub za pomocą poczty elektronicznej: **przetargi@ncbr.gov.pl**. W przypadku przekazywania oświadczeń, wniosków, zawiadomień i informacji za pomocą poczty elektronicznej każda ze stron jest zobowiązana na żądanie drugiej strony niezwłocznie potwierdzić fakt jej otrzymania.

8.2. W przypadku nie wywiązania się przez Wykonawcę ze wskazanego w pkt 8.1. powyżej obowiązku, Zamawiający uzna, że oświadczenia, wnioski, zawiadomienia oraz informacje dotarły do Wykonawcy w dniu i godzinie jego nadania oraz były czytelne.

8.3. Zamawiający nie ponosi odpowiedzialności z tytułu nieotrzymania przez Wykonawcę informacji związanych z prowadzonym postępowaniem w przypadku wskazania przez Wykonawcę w ofercie np. błędnego adresu, numeru faksu lub adresu poczty elektronicznej.

8.4. Wykonawca może na piśmie, faksem lub w formie elektronicznej zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SIWZ. Zamawiający niezwłocznie udzieli wyjaśnień jednak nie później niż **2 dni** przed terminem składania ofert – pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert i nie dotyczy udzielonych wyjaśnień.

Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania ww. wniosków. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynął po upływie terminu, o którym mowa powyżej lub dotyczy

udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.

8.5. Pytania należy przesyłać pisemnie na adres Zamawiającego lub za pomocą poczty elektronicznej na adres: przetargi@ncbr.gov.pl. Jako temat przesłanej wiadomości należy podać następującą treść: **18/20/PN/P24 – dostawa licencji na system ochrony infrastruktury IT dla NCBR**.

8.6. Treść zapytań wraz z wyjaśnieniami Zamawiający przekaże niezwłocznie wszystkim Wykonawcom, którym przekazał SIWZ, bez ujawniania źródła zapytania oraz zamieści na stronie internetowej Zamawiającego.

8.7. W szczególnie uzasadnionych przypadkach Zamawiający może w każdym czasie, przed upływem terminu składania ofert zmodyfikować treść niniejszej SIWZ.

8.8. Każda wprowadzona przez Zamawiającego zmiana SIWZ stanie się częścią SIWZ. Dokonaną zmianę treści SIWZ Zamawiający udostępni na stronie internetowej Zamawiającego.

8.9. Zamawiający przedłuży termin składania ofert, jeżeli w wyniku modyfikacji treści SIWZ niezbędny będzie dodatkowy czas na wprowadzenie zmian w ofertach.

8.10. O przedłużeniu terminu składania ofert Zamawiający niezwłocznie zawiadomi wszystkich Wykonawców, którym przekazał SIWZ oraz zamieści stosowną informację na stronie internetowej Zamawiającego.

9. WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający nie wymaga wniesienia wadium.

10. TERMIN ZWIĄZANIA OFERTĄ

10.1. Okres związania Wykonawcy ofertą wynosi 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

10.2. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni (art. 85 ust. 2 uPzp).

10.3. W przypadku wniesienia odwołania po upływie terminu składania ofert bieg terminu związania ofertą ulega zawieszeniu do czasu ogłoszenia orzeczenia przez Krajową Izbę Odwoławczą.

11. OPIS SPOSOBU PRZYGOTOWANIA OFERT

11.1. Zamawiający dopuszcza możliwość złożenia oferty w postaci elektronicznej lub w formie pisemnej. Wykonawca wybiera sposób złożenia oferty.

11.2. W postaci elektronicznej Wykonawca składa ofertę za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Klucz publiczny niezbędny do zaszyfrowania oferty przez Wykonawcę jest dostępny dla wykonawców na miniPortalu.

11.2.1. Oferta składana w postaci elektronicznej powinna być sporządzona w języku polskim, z zachowaniem postaci elektronicznej w jednym z następujących formatów danych: .pdf, .doc, .docx, .rtf, .xps, .odt, i podpisana kwalifikowanym podpisem elektronicznym.

11.2.2. Otwarcie ofert następuje poprzez użycie aplikacji do szyfrowania ofert dostępnej na miniPortalu i dokonywane jest poprzez odszyfrowanie i otwarcie ofert za pomocą klucza prywatnego.

11.2.3. Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty lub wniosku dostępnego na ePUAP i udostępnionych również na miniPortalu. Sposób zmiany i wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortalu.

11.2.4. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

11.2.5. Obowiązkiem Wykonawcy jest zapoznać się z Regulaminem korzystania z miniPortalu oraz Regulaminem ePUAP. W związku z powyższym złożenie ofert w sposób niezgodny z Regulaminem (np. podwójne zaszyfrowanie) może spowodować brak możliwości odczytania oferty, za co odpowiedzialność ponosi Wykonawca. W takim przypadku Zamawiający potraktuje ofertę, jako nie złożoną skutecznie. Zamawiający zaleca zapoznanie się z Załącznikiem nr 7 do SIWZ, który jest Skróconą instrukcja przygotowania i złożenia oferty na miniPortalu.

11.2.6. Zamawiający zaleca, aby zgodnie z wytycznymi Urzędu Zamówień Publicznych, Wykonawca zwracał uwagę na to, czy ID postępowania, które wpisuje do aplikacji do szyfrowania, zgadza się z kluczem publicznym.

11.2.7. W celu prawidłowego użycia pary kluczy do szyfrowania i deszyfrowania, oferta musi zostać zaszyfrowana tylko jeden raz. Podczas szyfrowania oferty system generuje hash pliku połączony z wygenerowanymi kluczami. W momencie podwójnego zaszyfrowania oferty, system miniPortal dostaje informację o hashu pliku wyłącznie zaszyfrowanego pliku po raz ostatni, który jest wysyłany poprzez formularze do złożenia, wycofania lub zmiany oferty. Przy odszyfrowaniu Aplikacja „sczytuje" tylko ten ostatni hash pliku. W związku z powyższym brak jest możliwości otwarcia podwójnie zaszyfrowanej oferty.

11.3. Ofertę w formie pisemnej składa się pod rygorem nieważności, podpisaną własnoręcznym podpisem lub Oferta musi być przygotowana w języku polskim, w sposób czytelny zgodnie z treścią Formularza oferty, którego wzór stanowi Załącznik nr 2 do SIWZ. Ofertę w formie pisemnej Wykonawca składa w siedzibie Zamawiającego zgodnie z opisem z pkt 12 i 13 SIWZ.

11.4. Do oferty należy dołączyć następujące oświadczenia i dokumenty:

11.4.1. oświadczenie, o którym mowa w pkt 7.1.1. sporządzone według wzoru stanowiącego Załącznik nr 3 do SIWZ;

11.4.2. pełnomocnictwo - jeśli dotyczy;

11.4.3. zobowiązanie podmiotu trzeciego, o którym mowa w pkt 7.1.5. powyżej – jeżeli Wykonawca polega na zasobach innego podmiotu;

11.5 Formularz oferty, oświadczenia Wykonawcy zaleca się sporządzić na drukach stanowiących załączniki do SIWZ.

11.6. W przypadku, gdy Wykonawca nie skorzysta z załączonego do SIWZ Formularza oferty (Załącznik nr 2 do SIWZ), zobowiązany jest on złożyć ofertę w taki sposób, by treść oferty odpowiadała treści SIWZ.

W przypadku, gdy Wykonawca nie skorzysta z załączonych druków (Załączniki nr 3-5 do SIWZ), treść składanych oświadczeń powinna potwierdzać spełnianie warunków udziału w postępowaniu oraz braku podstaw wykluczenia obowiązujących w niniejszym postępowaniu.

11.6 Formularz oferty, oświadczenie o którym mowa w pkt 7.1.1. SIWZ, zobowiązanie podmiotu, o którym mowa w pkt 5.7.1. SIWZ, oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w pkt 7.3. SIWZ oraz inne oświadczenia dotyczące Wykonawcy/Wykonawców występujących wspólnie i innych podmiotów, na których zdolnościach polega Wykonawca na zasadach określonych w art. 22a uPzp składane są w oryginale. Dokumenty inne niż oświadczenia składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem zgodnie z pkt 11.7. SIWZ.

Forma dokumentu pełnomocnictwa uregulowana jest w pkt 7.12. SIWZ.

11.8 Formularz oferty, oświadczenie określone w pkt 7.1.1. SIWZ, a także oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w pkt 7.3. SIWZ oraz inne oświadczenia dotyczące Wykonawcy/Wykonawców występujących wspólnie muszą być podpisane przez osobę(-y) upoważnioną(-e) do reprezentowania Wykonawcy/Wykonawców występujących wspólnie (tzn. zgodnie z formą reprezentacji określoną w odpowiednim rejestrze lub innym dokumencie właściwym dla formy organizacyjnej Wykonawcy/Wykonawców) bądź posiadającą(-ce) stosowne pełnomocnictwo, o którym mowa w pkt 7.11. SIWZ.

11.9 Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. By cel poświadczenia nie budził wątpliwości prosimy o następującą formułę na dokumencie „ZA ZGODNOŚĆ Z ORYGINAŁEM" na każdej zapisanej stronie bądź formułę „Poświadczam za zgodność z oryginałem strony od …. do …." oraz podpis(-y) osoby/osób upoważnionej(-ych) do reprezentacji odpowiednio Wykonawca, podmiot, na którego zdolnościach polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca. Poświadczenie za zgodność z oryginałem następuje w formie pisemnej. Powyższe nie odnosi się do poświadczeń notarialnych.

11.10 Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

11.11 Wykonawca w ofercie może zastrzec informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.). Zamawiający nie ujawni informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, **jeżeli Wykonawca, nie później niż w terminie składania ofert, zastrzegł, że nie mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Zaleca się, aby uzasadnienie, o którym mowa powyżej było sformułowane w sposób umożliwiający jego udostępnienie innym uczestnikom postępowania.**

Uwaga:

Zastrzegając informacje w ofercie Wykonawca winien mieć na względzie, że zastrzeżona informacja ma charakter tajemnicy przedsiębiorstwa, jeśli spełnia łącznie trzy warunki:

a) ma charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub posiada wartość gospodarczą,

b) nie została ujawniona do wiadomości publicznej tzn. nie jest znana ogółowi lub osobom, które ze względu na prowadzoną działalność są zainteresowane jej posiadaniem,

c) podjęto w stosunku do niej niezbędne działania w celu zachowania poufności.

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

Zamawiający zastrzega, że klauzulą tajności nie mogą być zastrzeżone w ofercie informacje podlegające ocenie. W przypadku objęcia ich tajemnicą przedsiębiorstwa Zamawiający dokona odtajnienia treści oferty w części podlegającej ocenie.

11.12 Zamawiający informuje, że w przypadku kiedy Wykonawca otrzyma od niego wezwanie w trybie art. 90 ustawy PZP, a złożone przez niego wyjaśnienia i/lub dowody stanowić będą tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji Wykonawcy będzie przysługiwało prawo zastrzeżenia ich, jako tajemnica przedsiębiorstwa. Przedmiotowe zastrzeżenie Zamawiający uzna za skuteczne wyłącznie w sytuacji kiedy Wykonawca oprócz samego zastrzeżenia, jednocześnie wykaże, iż dane informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

11.13 Wykonawca w szczególności nie może zastrzec w ofercie informacji:

11.13.1 odczytywanych podczas otwarcia ofert, o których mowa w art. 86 ust. 4 ustawy PZP,

11.13.2 które są jawne na mocy odrębnych przepisów,

11.13.3 cen jednostkowych stanowiących podstawę wyliczenia ceny oferty.

11.14 Wszelkie negatywne konsekwencje mogące wyniknąć z niezachowania powyższych wymagań będą obciążały Wykonawcę.

12. OPAKOWANIE I OZNAKOWANIE OFERT W FORMIE PAPIEROWEJ

12.1. Oferta powinna znajdować się w nieprzejrzystej kopercie, zapieczętowanej w sposób zapewniający zachowanie w poufności jej treści oraz zabezpieczającej jej nienaruszalność do terminu składania ofert. Koperta powinna być oznaczona nazwą i adresem Zamawiającego, nazwą i dokładnym adresem Wykonawcy oraz napisem: **„Oferta na dostawę licencji na system ochrony infrastruktury IT dla NCBR" Oznaczenie sprawy znak:18/20/PN/P24 oraz „NIE OTWIERAĆ PRZED DNIEM 06.05.2020 r. godz. 12.00".**

Konsekwencje złożenia oferty niezgodnie z ww. opisem (np. potraktowanie oferty, jako zwykłej korespondencji i nie dostarczenie jej na miejsce składania ofert w terminie określonym w SIWZ) ponosi Wykonawca. ***W przypadku składania oferty za pośrednictwem firmy kurierskiej zewnętrzne opakowanie oferty (np. firmowa koperta firmy kurierskiej) winno być również oznaczone w sposób umożliwiający przyporządkowanie oferty do niniejszego postępowania, tj. co najmniej nazwą lub numerem postępowania.***

Zamawiający zaleca, aby informacje zastrzeżone, jako tajemnica przedsiębiorstwa były przez Wykonawcę złożone w oddzielnej wewnętrznej kopercie z oznakowaniem „tajemnica przedsiębiorstwa", lub spięte (zszyte) oddzielnie od pozostałych, jawnych elementów oferty. Brak jednoznacznego wskazania, które informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania są jawne bez zastrzeżeń.

13. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

13.1. Ofertę w formie elektronicznej (t.j. w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) albo pisemnej (t.j. w postaci papierowej z własnoręcznym podpisem) wraz z wymaganymi załącznikami należy złożyć do dnia **06.05.2020 r do godz. 12.00**. Oferty otrzymane przez Zamawiającego po tym terminie zostaną zwrócone na zasadach określonych w art. 84 ust. 2 uPzp.

13.2. Ofertę w formie elektronicznej Wykonawca składa za pośrednictwem Formularza do złożenia oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób złożenia oferty opisany został w Instrukcji użytkownika dostępnej na miniPortalu.

13.3. Wykonawca po przesłaniu oferty za pomocą Formularza do złożenia oferty, na „ekranie sukcesu" otrzyma numer oferty generowany przez ePUAP. Ten numer należy zapisać i zachować. Będzie on potrzebny w razie ewentualnego wycofania oferty.

13.4. Ofertę w formie pisemnej należy złożyć w siedzibie Zamawiającego w biurze podawczym znajdującym się na parterze. Termin składania ofert upływa dnia **06.05.2020 r. do godziny 12.00**. Oferty otrzymane przez Zamawiającego po tym terminie zostaną zwrócone na zasadach określonych w art. 84 ust. 2 uPzp.

13.5. Decydujące znaczenie dla oceny zachowania terminu składania ofert ma data i godzina wpływu oferty do Zamawiającego, a nie data jej wysłania przesyłką pocztową czy kurierską.

13.6. Otwarcie ofert nastąpi w dniu, w którym upływa termin ich składania **tj. 06.05.2020r. o godz. 13.00** w siedzibie Zamawiającego w sali 237 (II piętro) oraz za pomocą kanału Zamawiającego na YouTube.

13.7. Wykonawca zgodnie z art. 84 ust. 1 ustawy PZP może przed upływem terminu do składania ofert, zmienić lub wycofać ofertę.

13.8. Wykonawca o wprowadzeniu zmian lub zamiarze wycofania oferty powiadamia Zamawiającego pisemnie.

13.9. Pismo informujące o zmianie lub wycofaniu oferty należy złożyć (przed terminem składania ofert) zgodnie z opisem podanym w pkt 12 powyżej, oznaczając dodatkowo: „ZMIANA OFERTY" lub „WYCOFANIE OFERTY".

13.10. Do pisma o wycofaniu lub zmianie oferty musi być załączony dokument, z którego wynika prawo osoby podpisującej informację do reprezentowania Wykonawcy/Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

14. INFORMACJA O TRYBIE OTWARCIA I OCENY OFERT

14.1. Otwarcie ofert jest jawne, Wykonawcy mogą w nim uczestniczyć, bądź oglądać za pomocą kanału YouTube w internecie.

14.2. Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

14.3. Podczas otwarcia ofert podaje się nazwy (firmy) oraz adresy wykonawców, a także informacje dotyczące ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach, zgodnie z art. 86 ust. 4 ustawy PZP. Niezwłocznie po otwarciu ofert, Zamawiający zamieści na stronie www.ncbr.gov.pl informacje dotyczące:

14.4.1. kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia;

14.4.2. firm oraz adresów Wykonawców, którzy złożyli oferty w terminie;

14.4.3. ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

14.5. W toku dokonywania badania i oceny złożonych ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących ich treści.

14.6. Oferty, które nie zostaną odrzucone, zostaną poddane procedurze oceny zgodnie z kryterium oceny ofert określonym w pkt 17 niniejszej SIWZ.

14.7. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w ustawie PZP oraz w SIWZ i uzyska największą liczbę punktów zgodnie z przyjętymi kryteriami oceny ofert.

15. OPIS SPOSOBU OBLICZANIA CENY

15.1. Cena oferty brutto jest ceną obejmującą wszystkie koszty i składniki związane z realizacją zamówienia (w tym m.in. podatek VAT, ewentualne upusty i rabaty).

15.2. Wykonawca w Formularzu oferty stanowiącym Załącznik nr 2 do SIWZ poda całkowitą wartość za wykonanie zamówienia.

15.3. Wszystkie ceny należy podać w złotych polskich. Wykonawca określi ceny za wszystkie elementy zamówienia, wypełniając odpowiednio wszystkie pola Formularza ofertowego.

15.4. Wszystkie ceny określone przez Wykonawcę zostaną ustalone na okres obowiązywania umowy i nie będą podlegały zmianom ani waloryzacji w okresie realizacji umowy.

15.5. Wszystkie wymienione wartości należy podać z dokładnością do dwóch miejsc po przecinku.

15.6. Cena oferty musi zostać wyrażona cyfrowo i słownie. W przypadku rozbieżności przyjmuje się cenę wyrażoną słownie. W formularzu oferty należy podać:

15.6.1. cenę oferty netto – bez podatku VAT,

15.6.2. cenę oferty brutto – łącznie z podatkiem VAT,

15.6.3. cenę netto odnowionych licencji – bez podatku VAT,

15.6.4. cenę brutto odnowionych licencji – z podatkiem VAT,

15.6.3. cenę netto nowo zakupionych licencji – bez podatku VAT,

15.6.4. cenę brutto nowo zakupionych licencji – z podatkiem VAT,

15.6.5. stawkę podatku VAT.

15.7. Ustalenie prawidłowej stawki podatku VAT leży po stronie Wykonawcy.

15.8. Zamawiający nie uzna za oczywistą omyłkę i nie poprawi błędnie ustalonej stawki podatku VAT.

15.9. Jeżeli w postępowaniu złożona będzie oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. **W takim przypadku Wykonawca, składając ofertę, jest zobligowany poinformować Zamawiającego, że wybór jego oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazać ich wartość bez kwoty podatku.**

16. INFORMACJE DOTYCZĄCE WALUT OBCYCH, W JAKICH MOGĄ BYĆ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ

16.1. W związku z wykonaniem umowy w sprawie zamówienia publicznego w przedmiotowym postępowaniu Zamawiający nie przewiduje prowadzenia rozliczeń z Wykonawcą w walutach obcych.

16.2. Rozliczenia pomiędzy Zamawiającym a Wykonawcą będą dokonywane w złotych polskich.

17. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM ZNACZENIA TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

17.1. Kryteria, którymi Zamawiający będzie się kierował przy wyborze oferty oraz odpowiadająca mu waga jest następująca:

Cena oferty - waga kryterium 100%,

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

Zamawiający dokona obliczenia stosując poniższy wzór:

$$LP = \frac{Cn}{Cb} * \text{WAGA WARIANTU}$$

gdzie:

LP = liczba uzyskanych punktów;

Cn = najniższa cena z ofert,

Cb = cena konkretnej badanej oferty,

WAGA WARIANTU = 100

17.2. Zamawiający odrzuci ofertę, jeżeli:

17.2.1. jest niezgodna z ustawą;

17.2.2. jej treść nie odpowiada treści SIWZ, z zastrzeżeniem art. 87 ust.2 pkt 3 ustawy PZP;

17.2.3. nie zawiera projektu graficznego do oceny;

17.2.4. jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;

17.2.5. zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia;

17.2.6. została złożona przez Wykonawcę wykluczonego z udziału w postępowaniu o udzielenie zamówienia;

17.2.7. zawiera błędy w obliczeniu ceny lub kosztu;

17.2.8. Wykonawca w terminie 3 dni od dnia doręczenia mu zawiadomienia nie zgodzi się na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3 ustawy PZP;

17.2.9. Wykonawca nie wyraził zgody, o której mowa w art. 85 ust. 2 uPzp, na przedłużenie terminu związania ofertą;

17.2.10. jest nieważna na podstawie odrębnych przepisów,

17.2.11. jako niezgodną z SIWZ, w przypadku gdy Wykonawca uchyli się od zawarcia umowy, co spowoduje zmianę treści złożonej przez niego oferty.

17.3. Jeżeli nie można będzie wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawi taki sam bilans ceny lub kosztu i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybierze ofertę z najniższą ceną lub najniższym kosztem, a jeżeli zostały złożone oferty o takiej samej cenie lub koszcie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych.

18. POPRAWIENIE OMYŁEK W OFERCIE

18.1. Zamawiający poprawi w ofercie, w szczególności:

18.1.1. **oczywiste omyłki pisarskie** – bezsporne, nie budzące wątpliwości omyłki dotyczące wyrazów, np.: widoczna mylna pisownia wyrazu, ewidentny błąd gramatyczny, niezamierzone opuszczenie wyrazu lub jego części, ewidentny błąd rzeczowy np.: 31 kwietnia 2013 r., rozbieżność pomiędzy ceną wpisaną liczbą i słownie;

18.1.2. **oczywiste omyłki rachunkowe** z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek – omyłki dotyczące działań arytmetycznych na liczbach, np.: błędny wynik działania matematycznego wynikający z dodawania, odejmowania, mnożenia i dzielenia;

18.1.3. **inne omyłki** - polegające na niezgodności oferty z SIWZ niepowodujące istotnych zmian w treści oferty.

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

19. INFORMACJA O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY O ZAMÓWIENIE PUBLICZNE ORAZ INFORMACJE ZAWARTE W ART. 92 UST. 1 USTAWY PZP

19.1. Umowa w sprawie wykonania zamówienia publicznego, którego przedmiot został określony w niniejszej SIWZ, zawarta zostanie z uwzględnieniem postanowień wynikających z treści niniejszej SIWZ oraz danych zawartych w ofercie.

19.2. Zamawiający podpisze umowę z Wykonawcą, który przedłoży najkorzystniejszą ofertę z punktu widzenia kryteriów przyjętych w niniejszej SIWZ.

19.3. Zamawiający informuje niezwłocznie wszystkich wykonawców o:

19.3.1. wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania i adres, jeżeli jest miejscem wykonywania działalności wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania i adresy, jeżeli są miejscami wykonywania działalności wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację,

19.3.2. wykonawcach, którzy zostali wykluczeni,

19.3.3. wykonawcach, których oferty zostały odrzucone, powodach odrzucenia oferty, a w przypadkach, o których mowa w art. 89 ust. 4 i 5, braku równoważności lub braku spełniania wymagań dotyczących wydajności lub funkcjonalności,

19.3.4. wykonawcach, którzy złożyli oferty niepodlegające odrzuceniu, ale nie zostali zaproszeni do kolejnego etapu negocjacji albo dialogu,

19.3.5. unieważnieniu postępowania

– podając uzasadnienie faktyczne i prawne.

19.4. Zamawiający określi datę i miejsce podpisania umowy. Termin podpisania umowy nie będzie krótszy niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni – jeżeli zostało przesłane w inny sposób.

19.5. Przed podpisaniem umowy wybrany Wykonawca przekaże Zamawiającemu informacje dotyczące wskazania osób podpisujących umowę oraz osoby upoważnione do kontaktów w sprawach realizacji umowy;

19.6. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający zastrzega sobie prawo żądania, przed podpisaniem umowy w sprawie udzielenia zamówienia publicznego, umowy regulującej współpracę tych Wykonawców.

19.7. O terminie i miejscu podpisania umowy Zamawiający poinformuje wybranego Wykonawcę odrębnym pismem lub drogą mailową.

19.8. Umowa zostanie zawarta w formie pisemnej.

19.9. Jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy w sprawie zamówienia publicznego, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert bez przeprowadzania ich ponownej oceny.

20. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

20.1. Zamawiający żąda od Wykonawcy wniesienia zabezpieczenia należytego wykonania umowy, które służy na pokrycie roszczeń z tytułu niewykonania lub nienależytego wykonania umowy w wysokości **5%** ceny całkowitej brutto podanej w ofercie.

20.2. Do dnia zawarcia umowy, Wykonawca jest obowiązany wnieść zabezpieczenie należytego wykonania umowy w całości.

20.3. Zabezpieczenie należytego wykonania umowy może być wnoszone według wyboru Wykonawcy w jednej lub w kilku następujących formach:

20.3.1. pieniądzu;

20.3.2. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo – kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;

20.3.3. gwarancjach bankowych;

20.3.4. gwarancjach ubezpieczeniowych;

20.3.5. poręczeniach udzielanych przez podmioty, o których mowa w art. 6 b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.

20.4 Zabezpieczenie należytego wykonania umowy wnoszone w:

20.4.1. pieniądzu Wykonawca wpłaca przelewem na następujący rachunek bankowy Zamawiającego:

Bank Gospodarstwa Krajowego I Oddział w Warszawie

22 1130 1017 0020 1020 9820 0001

z zaznaczeniem: „Zabezpieczenie – licencji na system ochrony infrastruktury IT dla NCBR”

20.4.2. w innej formie niż pieniądz - oryginał dokumentu potwierdzającego wniesienie zabezpieczenia należytego wykonania umowy musi być dostarczony do Zamawiającego przed podpisaniem umowy.

20.5 Zamawiający nie wyraża zgody na wniesienie zabezpieczenia należytego wykonania umowy w formach wymienionych w art. 148 ust. 2 ustawy Pzp.

20.6. Zamawiający 100% wysokości zabezpieczenia zwróci w terminie 30 (trzydziestu) dni kalendarzowych od dnia zakończenia okresu obowiązywania licencji na Oprogramowanie.

21. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI UMOWY

21.1. Istotne dla Stron postanowienia zostały zawarte w Istotnych postanowieniach Umowy. Istotne postanowienia Umowy stanowią Załącznik Nr 6 do SIWZ.

21.2. Złożenie oferty jest jednoznaczne z akceptacją wszystkich warunków zawartych we wzorze umowy.

22. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

22.1. Każdemu Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy PZP przysługują środki ochrony prawnej przewidziane w dziale VI ustawy PZP jak dla trybu przetargu nieograniczonego o wartości nieprzekraczającej 139 000 euro.

22.2. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz SIWZ przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt 5 ustawy PZP.

23. PODWYKONAWSTWO

23.1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy.

23.2. W przypadku powierzenia wykonania części zamówienia podwykonawcy, Zamawiający żąda wskazania przez Wykonawcę w ofercie (Formularzu oferty) części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, oraz podania przez Wykonawcę nazw (firm) podwykonawców.

23.3. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 22a ust. 1 ustawy, 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.

23.4. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie zamówienia.

24. OCHRONA DANYCH OSOBOWYCH

24.1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", Zamawiający informuje, że:

- administratorem Pani/Pana danych osobowych jest *Narodowe Centrum Badań i Rozwoju, ul. Nowogrodzka 47a, 00-695 Warszawa;*
- kontakt z inspektorem ochrony danych osobowych w *Narodowym Centrum Badań i Rozwoju* można uzyskać pod adresem inspektorochronydanychosobowych@ncbr.gov.pl;

  Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego ***18/20/PN/P24 na dostawę licencji na system ochrony infrastruktury IT dla NCBR*** w trybie przetargu nieograniczonego;
- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843 oraz z 2020 r. poz. 288.), dalej „ustawa PZP";

- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy PZP, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy PZP, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy PZP;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- posiada Pani/Pan:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych**;
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ***;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

Wykaz Załączników do niniejszego SIWZ:

1. Załącznik 1 – Szczegółowy opis przedmiotu zamówienia;
2. Załącznik 2 – Formularz oferty;
3. Załącznik 3 – Oświadczenia w zakresie braku podstaw wykluczenia;
4. Załącznik 4 – Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy PZP;
5. Załącznik 5 – Wykaz usług;
6. Załącznik 6 – Istotne postanowienia umowy;
7. Załącznik 7 – Skrócona instrukcja przygotowania i złożenia oferty.

Załącznik nr 1 do SIWZ

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:
   2.1. **McAfee Complete Data Protection Advanced – 100 szt.**
   2.2. **McAfee Threat Intelligence Exchange - 100 szt.**
   2.3. **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 2 do SIWZ

…….

Pieczęć firmowa Wykonawcy

FORMULARZ OFERTY

dla Narodowego Centrum Badań i Rozwoju

.....

PEŁNA NAZWA WYKONAWCY/WYKONAWCÓW

.....

ADRES Z KODEM POCZTOWYM

……..……..…

NR TELEFONU E-MAIL

....

NIP REGON

.....

IMIONA I NAZWISKA OSÓB UPOWAŻNIONYCH DO REPREZENTOWANIA I SKŁADANIA OŚWIADCZEŃ WOLI W IMIENIU WYKONAWCY

Oferta na dostawę licencji na system ochrony infrastruktury IT w NCBR oferujemy wykonanie przedmiotu zamówienia w pełnym rzeczowym zakresie ujętym w SIWZ za cenę:

Oświadczamy, że cena oferty jest ceną obejmującą wszystkie koszty i składniki związane z realizacją zamówienia (w tym m.in. ewentualne upusty i rabaty):

<u>Wartość oferty:</u>

Cena netto …….. zł (słownie: ……..)

wysokość stawki podatku VAT …….. %

wartość podatku VAT (cena netto x stawka VAT) …… zł

(słownie: ……)

Cena brutto ……. zł (słownie: ……)

W skład, której wchodzi:

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

   Licencja równoważna TAK/NIE*

   Nazwa równoważnej licencji: ……..

   Cena netto …….. zł (słownie: ……..)

   wysokość stawki podatku VAT …….. %

   wartość podatku VAT (cena netto x stawka VAT) …… zł

   (słownie: ……)

   Cena brutto ……. zł (słownie: ……)

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

   Licencja równoważna TAK/NIE*

   Nazwa równoważnej licencji: ……..

   Cena netto …….. zł (słownie: ……..)

   wysokość stawki podatku VAT …….. %

   wartość podatku VAT (cena netto x stawka VAT) …… zł

   (słownie: ……)

   Cena brutto ……. zł (słownie: ……)

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;

   Licencja równoważna TAK/NIE*

   Nazwa równoważnej licencji: ……..

   Cena netto …….. zł (słownie: ……..)

   wysokość stawki podatku VAT …….. %

wartość podatku VAT (cena netto x stawka VAT) …… zł

(słownie: ……)

Cena brutto ……. zł (słownie: ……)

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;

Licencja równoważna TAK/NIE*

Nazwa równoważnej licencji: ……..

Cena netto …….. zł (słownie: ……..)

wysokość stawki podatku VAT …….. %

wartość podatku VAT (cena netto x stawka VAT) …… zł

(słownie: ……)

Cena brutto ……. zł (słownie: ……)

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

Licencja równoważna TAK/NIE*

Nazwa równoważnej licencji: ……..

Cena netto …….. zł (słownie: ……..)

wysokość stawki podatku VAT …….. %

wartość podatku VAT (cena netto x stawka VAT) …… zł

(słownie: ……)

Cena brutto ……. zł (słownie: ……)

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

Licencja równoważna TAK/NIE*

Nazwa równoważnej licencji: ……..

Cena netto …….. zł (słownie: ……..)

wysokość stawki podatku VAT …….. %

wartość podatku VAT (cena netto x stawka VAT) …… zł

(słownie: ……)

Cena brutto ……. zł (słownie: ……)

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;

Licencja równoważna TAK/NIE*

Nazwa równoważnej licencji: ……..

Cena netto …….. zł (słownie: ……..)

wysokość stawki podatku VAT …….. %

wartość podatku VAT (cena netto x stawka VAT) …… zł

(słownie: ……)

Cena brutto ……. zł (słownie: ……)

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

Licencja równoważna TAK/NIE*

Nazwa równoważnej licencji: ……..

Cena netto …….. zł (słownie: ……..)

wysokość stawki podatku VAT …….. %

wartość podatku VAT (cena netto x stawka VAT) …… zł

(słownie: ……)

Cena brutto ……. zł (słownie: ……)

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

Licencja równoważna TAK/NIE*

Nazwa równoważnej licencji: ……..

Cena netto …….. zł (słownie: ……..)

wysokość stawki podatku VAT …….. %

wartość podatku VAT (cena netto x stawka VAT) …… zł

(słownie: ……)

Cena brutto ……. zł (słownie: ……)

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

    Licencja równoważna TAK/NIE*

    Nazwa równoważnej licencji: ……..

    Cena netto …….. zł (słownie: ……..)

    wysokość stawki podatku VAT …….. %

    wartość podatku VAT (cena netto x stawka VAT) …… zł

    (słownie: ……)

    Cena brutto ……. zł (słownie: ……)

Cena oferty brutto jest ceną obejmującą wszystkie koszty i składniki związane z realizacją zamówienia (w tym m.in. podatek VAT, koszty dostawy do siedziby Zamawiającego, ewentualne upusty i rabaty).

Nie wypełnienie pozycji ceny formularza oferty, bądź w przypadku licencji równoważnej nazwy, będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy PZP.

* **- zaznaczyć właściwą odpowiedź**

Oświadczamy, że:

1. zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia i nie wnosimy do niej zastrzeżeń ani do załączników będących integralną częścią SIWZ oraz, że uzyskaliśmy wszelkie informacje niezbędne do przygotowania oferty i podjęcia decyzji o jej złożeniu.
2. spełniamy wszystkie wymagania zawarte w SIWZ i w załącznikach będących integralną częścią SIWZ.
3. złożona przez nas oferta jest zgodna z treścią SIWZ i załącznikami będącymi integralną częścią SIWZ.
4. akceptujemy istotne postanowienia umowy, w tym warunki płatności oraz termin realizacji przedmiotu zamówienia podany przez Zamawiającego.

5. w przypadku wyboru naszej oferty, zobowiązujemy się w terminie i miejscu wyznaczonym przez Zamawiającego, do zawarcia umowy wg wzoru, stanowiącego Załącznik nr 6 do SIWZ.
6. uważamy się za związanych niniejszą ofertą 30 dni od dnia upływu terminu składania ofert;
7. oświadczamy, iż realizację przedmiotu zamówienia:

   w zakresie[2] …….

   powierzę(-my) podwykonawcy(-om), …… (nazwa podwykonawcy),po zawarciu stosownej umowy.
8. oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[3] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu
9. Informuję, iż dokumenty, o których mowa w pkt 7.6.2 SIWZ są dostępne w formie elektronicznej w ogólnodostępnych i bezpłatnych bazach danych pod adresem internetowym (jeżeli dotyczy):

   ……...

   (podać rodzaj dokumentu oraz adres strony internetowej)
10. Oferta została złożona na ……. stronach, ponumerowanych od nr … do nr …
11. Załącznikami do niniejszej oferty stanowiącymi jej integralną część są następujące dokumenty:
    a. .....
    b. .....
    c. .....
    d. .....

……

.....

miejscowość, data

podpis, imię i nazwisko

lub podpis na pieczęci imiennej

* Niepotrzebne skreślić

[2] Jeżeli Wykonawca zamierza powierzyć część prac podwykonawcy(-om) powinien wpisać powierzony zakres prac. W przypadku braku miejsca sporządzić stosowną informację w postaci załącznika do składanej oferty. Jeżeli Wykonawca nie zamierza powierzyć części prac podwykonawcy(-om) punktu tego może nie wypełniać lub wpisać nie dotyczy lub skreślić.

[3] rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1)

Załącznik nr 3 do SIWZ

Nazwa Wykonawcy w imieniu którego składane jest oświadczenie:

.....
.....
.....
.....
.....

Dotyczy: postepowania prowadzonego w trybie przetargu nieograniczonego na ***zakup licencji na system ochrony infrastruktury IT w NCBR.***

(oznaczenie sprawy 18/20/PN/P24)

OŚWIADCZENIE WYKONAWCY[4]

Niniejszym oświadczam, iż*:*

1) wobec podmiotu, który reprezentuję, nie wydano/wydano prawomocnego/ prawomocny wyroku/ wyrok sądu lub ostatecznej/ ostateczną decyzji/ decyzję administracyjnej/ administracyjną* o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne;
2) wobec podmiotu, który reprezentujemy, nie orzeczono/orzeczono tytułem środka zapobiegawczego zakazu/zakaz* ubiegania się o zamówienia publiczne.

* Niepotrzebne skreślić.

.....

data, podpis, imię i nazwisko lub podpis na pieczęci imiennej

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

Załącznik nr 4 do SIWZ

Nazwa Wykonawcy w imieniu którego składane jest oświadczenie:

.....
.....
.....
.....
.....

OŚWIADCZENIE [5]

w zakresie określonym w art. 24 ust. 11 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz.1843.), zwanej dalej „Pzp"

Niniejszym oświadczam(-my), iż [2]:

☐ nie należę(-my) do grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 Pzp

☐ należę(-my) do grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 Pzp i w załączeniu **przedstawiam dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia**.

.....

data, podpis, imię i nazwisko lub podpis na pieczęci imiennej

---

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

Załącznik nr 5 do SIWZ

…….

Pieczęć firmowa Wykonawcy

WYKAZ USŁUG

w zakresie niezbędnym do wykazania spełnienia warunku wiedzy i doświadczenia, o którym mowa w pkt 5.3.1. SIWZ, w okresie ostatnich 3 (trzech) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy, w tym okresie.

warunku udziału w postępowaniu określonego w art. 22 ust. 1b pkt 3 ustawy PZP (zdolności technicznej lub zawodowej): Wykonawcy winni wykazać, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wykonał należycie, a w przypadku świadczeń okresowych lub ciągłych wykonuje należycie co najmniej dwie dostawy licencji na oprogramowanie ochrony infrastruktury IT o wartości każdej z nich co najmniej **50 000,00 zł** (słownie: pięćdziesiąt tysięcy złotych) brutto;

Uwaga:

Zamawiający nie dopuszcza sumowania usług z różnych kontraktów w celu uzyskania wartości minimalnej.

Wykonawcy w celu wykazania spełnienia ww. warunków winni wykazać się realizacją minimum dwóch usług dla dwóch podmiotów.

Lp.	Wykonana usługa	
1	**Nazwa i zakres usługi**	…….. …….. tj. usługa polegająca na
	Data wykonania *(należy podać datę rozpoczęcia i zakończenia wskazanej usługi)*	od …..…/…..…./…..... do …..…/…..…./…..... *(dzień / miesiąc / rok)*
	Odbiorca (podmiot, który zlecał wykonanie usługi)	..…….……..…… …….……..……. *(nazwa i adres*)

	Dokument potwierdzający należyte wykonanie wyżej wymienionej usługi	Nr strony oferty - ……..……
2	**Nazwa i zakres usługi**	…….. …….. tj. usługa polegająca na.
	Data wykonania *(należy podać datę rozpoczęcia i zakończenia wskazanej usługi)*	od …..…/…..…./…..... do …..…/…..…./…..... *(dzień / miesiąc / rok)*
	Odbiorca (podmiot, który zlecał wykonanie usługi)	……..……..…… ……..……..……. *(nazwa i adres*)
	Dokument potwierdzający należyte wykonanie wyżej wymienionej usługi	Nr strony oferty - ……..……

Do powyższego wykazu załączam dowody potwierdzające, że wskazane w nim usługi, o których mowa w pkt 5.3.1. SIWZ, zostały wykonane należycie.

…… ……

miejscowość, data

podpis, imię i nazwisko
lub podpis na pieczęci imiennej

Załącznik nr 6 do SIWZ

WZÓR UMOWY

(osobny plik)

Załącznik nr 7 do SIWZ

SKRÓCONA INSTRUKCJA PRZYGOTOWANIA I ZŁOŻENIA OFERTY

Jeżeli jesteś Wykonawcą, który chce złożyć ofertę:

1. Upewnij się, że dysponujesz kontem na Platformie ePUAP. Jeśli nie – załóż konto dla podmiotu składającego ofertę. Konto to będzie potrzebne do przesłania oferty do Zamawiającego za pomocą narzędzia do składania ofert czyli tzw. miniPortalu. Adres Platformy ePUAP https://epuap.gov.pl/wps/portal;
2. Upewnij się, że osoby upoważnione do reprezentowania Wykonawcy, czyli te, które będą podpisywały ofertę dysponują ważnym kwalifikowanym podpisem elektronicznym. Będzie on niezbędny do podpisania oferty i innych oświadczeń oraz dokumentów składanych w postępowaniu.
3. Wypełnij formularz oferty, koniecznie w formie elektronicznej, czyli na komputerze (nie odręcznie).
4. Podpisz wypełniony formularz oferty (plik elektroniczny) kwalifikowanym podpisem elektronicznym osób upoważnionych do reprezentowania wykonawcy.

Procedura podpisu - wybierasz jeden lub więcej plików (możesz od razu podpisać wszystkie pliki do złożenia w postępowaniu), klikasz na przycisk uruchamiający procedurę podpisu i podajesz PIN, który ustanowiłeś dla swojego podpisu.

Na koniec powinieneś otrzymać komunikat, czy rzeczywiście procedura podpisu zakończyła się powodzeniem. Możesz też samodzielnie zweryfikować podpisane pliki, czy rzeczywiście zostały podpisane.

Zazwyczaj podpis elektroniczny pojawia się jako dodatkowy plik w folderze, w którym widnieje podpisywany dokument. Pamiętaj, że sam dokument bez pliku podpisu nie zostanie odczytany jako podpisany przez Ciebie. Potrzebujesz i pliku z dokumentem, i pliku z podpisem do tego dokumentu.

W przypadku formatu PDF podpis zazwyczaj jest zapisywany w samym pliku. Oznacza to, że nie pojawi Ci się dodatkowy plik z podpisem, lecz jest on dodany już do samego pliku PDF. Taki podpis jest też widoczny standardowo przy każdym otworzeniu takiego pliku.

5. Podpisany plik formularza oferty oraz podpisany plik Załącznika nr 3 do SIWZ. Oczywiście jeśli uważasz, że konieczne jest dołączenie do oferty innej zawartości jest to zawsze możliwe.
6. Spakuj pliki elektroniczne składające się na ofertę do jednego folderu skompresowanego (pliku) zarchiwizowanego w formacie ZiP.

Zaznacz wszystkie plik składane zamawiającemu – wszystkie składane pliki dokumentów oraz pliki podpisu tych dokumentów.

Kliknij na jeden z tych zaznaczonych plików prawym przyciskiem myszy – otworzy Ci się menu z wyborem poleceń.

Wybierz „Wyślij do”, a następnie „Folder skompresowany (zip)” – pojawi się nowy plik w formacie ZIP zawierający wszystkie zaznaczone przez Ciebie pliki (polecenia Windows 8, w innych wersjach tego systemu figurują one pod zbliżonymi nazwami).

Zmień nazwę swojego pliku ZIP na jakąś czytelną dla Ciebie np. „podpisana oferta ……..”.

Na etapie przesyłania oferty będziesz miał możliwość załączenia tylko jednego pliku – stąd konieczność stworzenia pliku ZIP – o rozmiarze do 150 MB.

7. Jeśli jeszcze nie dysponujesz, pobierz i zainstaluj aplikację do szyfrowania ofert. Aplikację możesz pobrać tu: https://miniportal.uzp.gov.pl/AplikacjaSzyfrowanie.aspx

8. Folder skompresowany (plik) zawierający składniki oferty, czyli minimum formularz oferty, formularz JEDZ i dokument potwierdzający wniesienie wadium, zaszyfruj za pomocą aplikacji do szyfrowania. Będziesz potrzebował do tego identyfikator postępowania i klucz publiczny. Klucz publiczny zamawiający dołączył do dokumentów postepowania. Dodatkowo informacje te znajdziesz i pozyskasz na Liście postepowań miniPortalu https://miniportal.uzp.gov.pl/ListaPostepowan.aspx (klucz publiczny i identyfikator postępowania w szczegółach dotyczących postepowania).

Uwaga! Nie otwieraj sam pliku z kluczem publicznym. Może ona wówczas zostać zapisany w zmienionym formacie i już go nie wykorzystasz do szyfrowania. W razie takich problemów pobierz po prostu klucz ponownie.

Uruchom aplikację szyfrującą Miniportalu, a następnie wybierze opcję: „Wykonawca (szyfrowanie ofert)". W celu zaszyfrowania oferty podaj aplikacji identyfikator postępowania oraz wybierz swój plik z ofertą, a także wybierz miejsce na dysku, gdzie zapisałeś klucz publiczny postępowania. Kliknij przycisk „szyfruj".

Następnie wyskoczy Ci okno, w którym będziesz mógł wybrać, gdzie chcesz zapisać plik z zaszyfrowaną ofertą oraz będziesz musiał wpisać jego nazwę. To ważne. Wpisz nazwę, z której będzie wynikało, że plik jest już zaszyfrowany np. „zaszyfrowana oferta na ……".

Powinieneś otrzymać informację o poprawnym zaszyfrowaniu pliku, a nowy plik ZIP pojawi się w wybranej przez Ciebie lokalizacji.

Oferta jest już gotowa do złożenia. Pozostało jedynie przekazanie jej zamawiającemu.

9. Wejdź na stronę https://obywatel.gov.pl/nforms/ezamowienia i wybierz „Formularz do złożenia, zmiany, wycofania oferty lub wniosku". Wypełnienie formularza i przesłanie go wraz z ofertą będzie wymagało konta na ePUAP. Nie musi to być konto podmiotu składającego ofertę, ale trzeba być przygotowanym, że zamawiający mógł przewidzieć dalsze prowadzenie korespondencji w postępowaniu przy pomocy platformy ePUAP, więc konto to musi być dla Ciebie dostępne.

Na platformie ePUAP musisz wykonać następujące czynności:

Podać dane identyfikacyjne postępowania – numer ogłoszenia znajdziesz na ogłoszeniu o zamówieniu, ale również na stronie postępowania na Miniportalu.

Uzupełnić dane formularza, czyli swoje dane oraz nazwę skrzynki ePUAP zamawiającego.

W kolejnym kroku formularza dodać jako załącznik swoją zaszyfrowaną ofertę. Nie musisz wpisywać swoich uwag.

Ostatni krok formularz to podgląd wniosku. Sprawdź wszystkie informacje, a następnie wyślij wniosek.

Powinieneś zostać przekierowany do strony z potwierdzeniem złożenia oferty. Widnieje na niej identyfikator potwierdzenia złożenia oferty. Skopiuj sobie ten numer. Bez niego nie uda Ci się zmienić lub wycofać oferty w przypadku takiej potrzeby.

Pamiętaj, że Twoja zaszyfrowana oferta jest od razu przekazywana zamawiającemu. Tym samym zamawiający widzi, że otrzymał ofertę w postępowaniu, z jakiej skrzynki została wysłana oraz jaka jest nazwa pliku z ofertą.

UWAGA

W celu prawidłowego użycia pary kluczy do szyfrowania i deszyfrowania, oferta musi zostać zaszyfrowana tylko jeden raz. Podczas szyfrowania oferty system generuje hash pliku połączony z wygenerowanymi kluczami. W momencie podwójnego zaszyfrowania oferty, system miniPortal dostaje informację o hashu pliku wyłącznie zaszyfrowanego pliku po raz ostatni, który jest wysyłany poprzez formularze do złożenia, wycofania lub zmiany oferty. Przy odszyfrowaniu Aplikacja „sczytuje" tylko ten ostatni hash pliku. W związku z powyższym brak jest możliwości otwarcia podwójnie zaszyfrowanej oferty.