Załącznik nr 8 do SIWZ

UMOWA
/PROJEKT/

Zawarta w dniu ……. 2019 r. w Łodzi pomiędzy:

Łódzkim Oddziałem Wojewódzkim Narodowego Funduszu Zdrowia
z siedzibą w Łodzi, przy ul. Kopcińskiego 58, 90-032 Łódź,
będącym płatnikiem podatku VAT, NIP 107-00-01-057,
reprezentowanym przez:
……...…….
zwanym dalej **Zamawiającym**,
a
……...……,
z siedzibą w ……...……...,
wpisanym do ……..……...……,
będącym płatnikiem podatku VAT, NIP: ……, REGON: ..…….……..……..…..,
reprezentowanym przez:
……...,
zwanym dalej **Wykonawcą,**

wybranym w wyniku postępowania o udzielenie zamówienia publicznego nr ZP/ŁOW NFZ/6/2019 prowadzonym w trybie przetargu nieograniczonego na podstawie przepisów ustawy Prawo zamówień publicznych z dnia 29 stycznia 2004 r. (t.j. Dz. U z 2019 r. poz. 1843) o następującej treści:

§ 1

1. Przedmiotem umowy jest sprzedaż, dostarczenie i wdrożenie systemu informatycznego wspomagającego ochronę danych w postaci elektronicznej przed utratą i wyciekami danych, dalej „system DLP", zgodnie z wymaganiami Zamawiającego zawartymi w specyfikacji istotnych warunków zamówienia, dalej „SIWZ, oraz w ofercie Wykonawcy z dnia …….. 2019 r.
2. Przedmiot umowy będzie realizowany zgodnie ze szczegółowym opisem przedmiotu zamówienia zawartym w **załączniku nr 1** do umowy, a także SIWZ.
3. Realizacja przedmiotu umowy nastąpi w terminie do 15 stycznia 2020 r. od dnia podpisania umowy.
4. Sporządzenie projektu technicznego, instalacja i wdrożenie systemu DLP, przekazanie dokumentacji powykonawczej oraz przeprowadzenie instruktażu dla pracowników Zamawiającego, dalej „instruktażu" z zakresu obsługi wdrożonego Systemu nastąpi w terminie określonym w ust. 3.
5. W dniu podpisania umowy Wykonawca dostarczy Zamawiającemu plan techniczny, zawierający szczegółowy harmonogram prac instalacyjnych dostarczonego systemu, procedurę instalacji oprogramowania oraz instruktażu.
6. Przedstawiony plan techniczny ma być zaakceptowany przez Zamawiającego, któremu przysługuje uprawnienie zgłoszenia do niego uwag. W terminie do 5 dni roboczych od dnia podpisania umowy Zamawiający ma ostatecznie zaakceptować plan techniczny, z wyłączeniem przypadku, gdy Zamawiający zgłosił uwagi do planu technicznego, a Wykonawca nie wprowadził poprawek w wyznaczonym terminie.

7. Dostarczone licencje/sublicencje systemu i wsparcie będą uprawniać Zamawiającego do pobierania poprawek, aktualizacji i nowych wersji systemu przez okres przynajmniej 12 miesięcy od dnia dostarczenia w sposób nienaruszający praw twórców i właściciela praw autorskich oraz nieograniczający praw Zamawiającego do korzystania z tego Oprogramowania zgodnie z celem umowy.
8. Przez pojęcie „licencja/sublicencja" Zamawiający rozumie prawo do legalnego korzystania z systemu, o którym mowa w § 1 ust. 1, na warunkach wskazanych przez producenta tego systemu oraz na warunkach wskazanych w umowie.
9. Przez system należy rozumieć kompleksowe rozwiązanie informatyczne dostarczane w ramach i zgodnie z umową.

§ 2

1. Wykonawca zobowiązuje się wykonać umowę zgodnie z obowiązującymi przepisami, treścią i jej celem, przy zachowaniu najwyższej staranności, uwzględniając zawodowy charakter prowadzonej działalności, zgodnie z zasadami współczesnej wiedzy technicznej i stosowanymi normami technicznymi, dobrymi praktykami i regułami.
2. Wykonawca ponosi pełną odpowiedzialność za wykonanie przedmiotu umowy.
3. W celu umożliwienia Wykonawcy wywiązania się ze swoich zobowiązań, Zamawiający zobowiązuje się w zakresie wymaganym dla prawidłowej realizacji umowy:
   3.1 współdziałać z Wykonawcą przy wykonywaniu umowy,
   3.2 na bieżąco zgłaszać Wykonawcy problemy związane z realizacją przedmiotu umowy.
4. Wykonawca oświadcza i gwarantuje, że:
   4.1 posiada wiedzę, doświadczenie, urządzenia i narzędzia, w tym informatyczne niezbędne do prawidłowego wykonania umowy,
   4.2 personel Wykonawcy wykonujący prace w ramach realizacji umowy posiada doświadczenie i kwalifikacje niezbędne do prawidłowego wykonania umowy.
5. Wykonawca zobowiązuje się w szczególności do:
   5.1 działania jedynie w zakresie swoich uprawnień i przestrzegania wskazówek Zamawiającego,
   5.2 przestrzegania obowiązujących przepisów o ochronie danych osobowych oraz ochronie informacji prawnie chronionych,
   5.3 odtworzenia utraconych, uszkodzonych lub zmienionych, w wyniku działania Wykonawcy danych i programów,
   5.4 delegowania dedykowanego zespołu osób do realizacji umowy,
   5.5 wykonania umowy w sposób niepowodujący zaprzestania lub zakłócenia pracy Zamawiającego,
   5.6 udostępnienia na każde żądanie Zamawiającego dokumentacji związanej z realizacją przedmiotu umowy.

§ 3

1. Wykonawca oświadcza i gwarantuje, że:
   1) dysponuje odpowiednią wiedzą, doświadczeniem i personelem niezbędnym do należytego wykonania zobowiązań wynikających z niniejszej umowy,
   2) wykona przedmiot umowy zgodnie z obowiązującymi przepisami i normami, w sposób profesjonalny, z uwzględnieniem najlepszych praktyk.
2. Wykonawca zobowiązuje się do zapewnienia we własnym zakresie i w ramach wynagrodzenia, o którym mowa w § 5 ust. 1 umowy wszystkich ewentualnych pozwoleń, zgód, certyfikatów wymaganych przez obowiązujące przepisy prawa w zakresie niezbędnym do prawidłowej realizacji umowy.

3. Wykonawca zapewnia, że w wyniku zawarcia umowy nie dojdzie do naruszenia praw osób trzecich. W przypadku zgłoszenia wobec Zamawiającego roszczeń o naruszenie praw osób trzecich, Wykonawca podejmie na swój koszt wszelkie środki obrony Zamawiającego przed takimi roszczeniami lub zarzutami i spowoduje, że Zamawiający będzie od nich zwolniony, a także pokryje wszelkie szkody, jakie poniesie Zamawiający z tego tytułu.
4. Wykonawca jest uprawniony do powierzenia wykonania umowy podwykonawcom, z zastrzeżeniem poniższych postanowień.
5. Wykonawca jest odpowiedzialny za działania, uchybienia i zaniedbania podwykonawców i jego pracowników w takim samym stopniu, jakby to były uchybienia lub zaniedbania jego własnych pracowników.
6. Wykonawca ponosi wyłączną odpowiedzialność za zapłatę wynagrodzenia podwykonawcom.
7. Wykonawca wykona przedmiot umowy przy udziale następujących podwykonawców:
   7.1 (wskazanie firmy, danych kontaktowych, osób reprezentujących podwykonawcę) …….- w zakresie…… *(jeżeli dotyczy).*
8. Wykonawca zobowiązany jest do poinformowania Zamawiającego w formie pisemnej o każdej zmianie danych dotyczących podwykonawców, jak również o ewentualnych nowych podwykonawcach, którym zamierza powierzyć prace w ramach realizacji umowy w terminie jednego dnia roboczego od dokonania zmiany.

§ 4

1. Wykonawca w ramach przysługującego mu wynagrodzenia, o którym mowa w § 5 ust. 1 umowy dostarczy Zamawiającemu przedmiot umowy na własny koszt i ryzyko.
2. Potwierdzeniem odbioru przedmiotu umowy będzie podpisany bez zastrzeżeń przez obie Strony Protokół odbioru, którego wzór stanowi **załącznik nr 2** do umowy.
3. Wykonawca zawiadomi Zamawiającego o terminie dostawy przedmiotu umowy najpóźniej na 24 godziny przed planowanym terminem dostawy.
4. Wykonawca musi zapewnić, aby wszystkie czynności odbiorcze przedmiotu umowy w tym również dotyczące przeprowadzenia instruktażu i podpisanie Protokołu odbioru, zostały zakończone w terminie określonym w § 1 ust. 3 umowy.
5. Do zaoferowanego systemu Wykonawca zobowiązuje się dostarczyć Zamawiającemu do jego siedziby: nośnik z wersją instalacyjną systemu, dane dostępowe do pobrania systemu (w przypadku systemu w formie elektronicznej lub objętego subskrypcją), licencje/sublicencje (umowy licencyjne w wersji papierowej lub elektronicznej w języku polskim lub angielskim) oraz wszystkie wymagane klucze licencyjne i aktywacyjne, instrukcje obsługi. W przypadku dostarczania licencji w formie elektronicznej należy je przesłać na adres: .....@nfz-lodz.pl. W przypadku rejestracji systemu drogą elektroniczną przez Wykonawcę należy użyć adresu poczty elektronicznej: .....@nfz-lodz.pl oraz danych adresowych Zamawiającego jeśli takowe będą wymagane.
6. W przypadku gdy Zamawiający stwierdzi, że dostarczone licencje/sublicencje nie pozwalają na korzystanie z systemu, zgodnie z umową i ogólnymi warunkami Producenta (w tym również ze względu na wady nośnika, na którym zostały przekazane), lub Wykonawca nie dostarczy ogólnych warunków Producenta, Zamawiający odmówi podpisania Protokołu odbioru, a Wykonawca ponownie dostarczy nośniki Oprogramowania wraz z Dokumentacją, Licencją oraz ogólnymi warunkami na swój koszt i ryzyko w terminie 4 dni roboczych, licząc od daty otrzymania od Zamawiającego zawiadomienia o stwierdzonej nieprawidłowości.
7. Z chwilą podpisania przez Zamawiającego bez zastrzeżeń Protokołu odbioru, na Zamawiającego przechodzi prawo własności do przekazanego egzemplarza dokumentacji oraz do nośnika, na którym został utrwalony system.

§ 5

1. Za wykonanie przedmiotu umowy określonego w § 1 Wykonawca otrzyma od Zamawiającego wynagrodzenie w kwocie brutto ……. zł (słownie złotych: …….).
2. Wynagrodzenie, o którym mowa w ust. 1, obejmuje wszystkie koszty związane z realizacją przedmiotu umowy, niezbędne do wykonania przedmiotu umowy, w tym wynagrodzenie za przeniesienie autorskich praw majątkowych oraz prawa zezwalania na wykonywanie praw zależnych do utworów, wynagrodzenie za udzielenie licencji na zasadach określonych w umowie. Wynagrodzenie określone w ust. 1 wyczerpuje wszelkie roszczenia finansowe Wykonawcy z tytułu realizacji umowy.
3. Wypłata wynagrodzenia określonego w ust. 1, nastąpi w terminie 7 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT, przelewem na rachunek bankowy Wykonawcy …….
4. Podstawą do wystawienia faktury VAT będzie podpisany przez strony protokół odbioru potwierdzający prawidłowość wykonania przedmiotu umowy, o którym mowa w § 4 ust. 2 umowy. Wraz z protokołem odbioru Wykonawca ma dostarczyć dokumentację powykonawczą dla wdrożonego systemu DLP.
5. Faktura wystawiona będzie na:
   - Nabywca: Narodowy Fundusz Zdrowia ul. Grójecka 186, 02-390 Warszawa, NIP: 107-000-10-57;
   - Odbiorca-płatnik: Łódzki Oddział Wojewódzki NFZ, ul. Kopcińskiego 58, 90-032 Łódź;

   i przesłana na adres Odbiorcy-płatnika.

§ 6

1. Wykonawca oświadcza i gwarantuje, że jakiekolwiek utwory w rozumieniu art. 1 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych oraz licencje przekazane Zamawiającemu w trakcie realizacji umowy, ani korzystanie z nich przez Zamawiającego lub inne podmioty zgodnie z umową, nie będą naruszać praw własności intelektualnej osób trzecich, w tym praw autorskich, patentów ani praw do baz danych.
2. Wykonawca oświadcza, że posiada uprawnienia niezbędne do korzystania z utworów przekazanych Zamawiającemu w trakcie realizacji umowy.
3. Wykonawca oświadcza i gwarantuje, iż w ramach wynagrodzenia brutto wskazanego w § 5 ust. 1 umowy z chwilą podpisania przez Strony protokołu odbioru udzielone zostają przez producenta Oprogramowania lub podmiot przez niego upoważniony bezterminowe, niewyłączne, rozciągające się na całe terytorium Rzeczypospolitej Polskiej, licencje na korzystanie z Oprogramowania, w szczególności na następujących polach eksploatacji:
   1) wprowadzenie i zapisywanie do pamięci komputera;
   2) odtwarzanie;
   3 przechowywanie;
   4) wyświetlanie;
   5) przystosowywanie;
   6) instalowanie i deinstalowanie Oprogramowania pod warunkiem zachowania udzielonych licencji;
   7) korzystanie na wszystkich polach funkcjonalności;
   8) korzystanie i modyfikowanie dokumentów oraz danych wykorzystywanych przy pomocy oprogramowania.
4. Wykonawca dostarcza licencje Oprogramowania wraz z dokumentacją producenta niezbędną do korzystania z Oprogramowania.

5. Dostarczone Licencje muszę być wystawione na Zamawiającego.
6. Licencje, o których mowa w umowie udzielone zostaną na warunkach producenta Oprogramowania, o ile umowa nie stanowi inaczej.
7. Dostarczone przez Wykonawcę licencje muszą zapewniać pełną i prawidłową realizację celu umowy, zamierzonego przez Zamawiającego.
8. Wykonawca oświadcza i gwarantuje, że jeżeli nie jest producentem Oprogramowania, to uzyskał zgodę producenta lub podmiotu upoważnionego przez producenta na korzystanie z Oprogramowania na zasadach określonych w umowie, w tym na przekazywanie dokumentów zawierających warunki licencji.
9. Wykonawca oświadcza i gwarantuje, że licencje na Oprogramowanie nie zostaną wypowiedziane, za wyjątkiem istotnego naruszenia przez Zamawiającego warunków licencji. W przypadku wypowiedzenia licencji na Oprogramowanie pomimo braku istotnego naruszenia warunków licencji przez Zamawiającego, Wykonawca odpowiadać będzie za wynikłą z tego tytułu szkodę oraz w ramach wynagrodzenia, o którym mowa w § 5 ust. 1 umowy dostarczy odpowiednie licencje odpowiadające warunkom zawartym w umowie i **załączniku nr 1** do umowy.
10. Z chwilą udzielenia licencji na Oprogramowanie własność nośników, na których je utrwalono przechodzi na Zamawiającego.
11. Jeżeli Zamawiający poinformuje Wykonawcę o jakichkolwiek roszczeniach osób trzecich zgłaszanych wobec Zamawiającego w związku z Oprogramowaniem, w tym zarzucających naruszenie praw własności intelektualnej, Wykonawca podejmie wszelkie działania mające na celu zażegnanie sporu i będzie zobowiązany naprawić każdą szkodę, za którą Zamawiający może stać się odpowiedzialny, lub do której naprawienia może zostać Zamawiający zobowiązany oraz poniesie w związku z tym wszelkie koszty, w tym koszty zastępstwa procesowego od chwili zgłoszenia roszczenia oraz koszty odszkodowań.
12. W przypadku wystąpienia osób trzecich wobec Zamawiającego z roszczeniami opartymi na twierdzeniu, iż używane przez Zamawiającego Oprogramowanie nie jest produktem wykonanym przez Producenta, Zamawiającemu przysługują wszystkie niżej wymienione uprawnienia, które ma prawo zrealizować według swojego wyboru (łącznie lub każde z osobna):
    1) prawo odstąpienia od umowy z wyłączeniem zapłaty na rzecz Wykonawcy jakichkolwiek kosztów, wynagrodzeń, odszkodowań itp.,
    2) zapłaty przez Wykonawcę na rzecz Zamawiającego kary umownej w wysokości 20% łącznej kwoty wynagrodzenia brutto określonego w § 5 ust. 1 umowy,
    3) prawo żądania odszkodowania uzupełniającego na zasadach ogólnych kc.

§ 7

1. Osobami sprawującymi nadzór nad realizacją umowy oraz upoważnionymi do podpisywania protokołów odbioru są:
    1) ze strony Zamawiającego: ……, tel. ……, e-mail ……..,
    2) ze strony Wykonawcy: …….……, tel. ……, e-mail …….……..
2. Osoby wymienione w ust. 1 odpowiedzialne są merytorycznie za nadzór nad prawidłowością i terminowością realizacji umowy, w szczególności upoważnione są do monitorowania należytego wykonania umowy oraz podpisania Protokołu odbioru.
3. Zmiana osób wskazanych w ust. 1 oraz ich danych kontaktowych nie wymaga zmiany umowy, a jedynie poinformowania drugiej Strony w formie pisemnej. Zawiadomienie takie powinno zostać podpisane przez osoby uprawnione do reprezentacji Stron.

§ 8

1. Wykonawca zapewni prawidłowe i sprawne działanie wdrożonego systemu DLP jako całości, jak również każdego z elementów tego systemu oddzielnie i udzieli ……. miesięcy gwarancji na system i wszystkie jego elementy (zgodnie z oświadczeniem Wykonawcy zawartym w formularzu Ofertowym).
2. Wykonawca zapewni również …….. miesięczne wsparcie serwisowe dla dostarczonego rozwiązania, które będzie świadczone przez Wykonawcę, w ramach wynagrodzenia przysługującego Wykonawcy na podstawie niniejszej umowy (zgodnie z oświadczeniem Wykonawcy zawartym w formularzu Ofertowym).
3. Zgłoszenia dotyczące wystąpienia wad, awarii mogą być przyjmowane pisemnie, telefonicznie, za pomocą faksu lub poczty elektronicznej: adres producenta: …...……..…, nr tel./faks: ……...…….., adres e-mail: ……
4. W okresie gwarancji Wykonawca jest zobowiązany w ramach przysługującego mu na podstawie niniejszej umowy wynagrodzenia, do wspierania wdrożonego systemu, co obejmuje również aktualizację systemu na następujących zasadach:
   1) konsultacje techniczne (telefoniczne lub mailowe typu hot-line) dostępne w dni robocze, przez minimum 8 godzin dziennie (od 8:00 do 16:00);
   2) usunięcie zgłoszonych wad/awarii w czasie 72h licząc od momentu zgłoszenia wady/awarii.
5. Przyjmuje się, że Zamawiający zgłosił wadę skutecznie, jeżeli wysłał jej skrócony opis i wezwanie do jej usunięcia do Wykonawcy pocztą elektroniczną (na adres wskazany przez Wykonawcę). Wykonawca zobowiązuje się do zwrotnego potwierdzenia przyjęcia zgłoszenia wady.
6. Zgłaszanie wad musi być możliwe w trybie 8 godzin x 5 dni w tygodniu.
7. Bieg terminu gwarancji rozpoczyna się od daty odbioru końcowego o którym mowa w § 4 ust. 2 niniejszej umowy.
8. W okresie gwarancji Wykonawca zobowiązuje się do bezpłatnego usunięcia stwierdzonych wad.
9. Gwarancja obejmuje wszelkie wady z wyjątkiem uszkodzeń mechanicznych, wad spowodowanych niewłaściwym lub niezgodnym z instrukcją obsługi użytkowaniem produktu oraz wad spowodowanych zdarzeniami losowymi.
10. Jeżeli usunięcie ujawnionej wady wdrożonego systemu jest możliwe wyłącznie w drodze dokonania zakupu jakichkolwiek udoskonaleń (w tym: unowocześnień, upgread'dów, dodatków sprzętowych, wszelkiego rodzaju usług, serwisów, licencji i uprawnień), Wykonawca jest zobowiązany dokonać tego zakupu na własny koszt i zainstalować przedmiot zakupu we wdrożonym systemie.
11. Wykonawca pokrywa w ramach gwarancji wszelkie koszty napraw i wymiany elementów systemu, w tym koszty dojazdu, transportu, demontażu, montażu, odinstalowania lub zainstalowania.
12. Udzielona przez Wykonawcę gwarancja nie wyłącza uprawnień Zamawiającego wynikających z rękojmi za wady oraz uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producenta sprzętu lub oprogramowania.
13. Wszelkie naprawy gwarancyjne jak i serwisowanie systemu muszą odbywać się w siedzibie Zamawiającego. Zakres gwarancji określony będzie w kartach gwarancyjnych i innych dokumentach, które Wykonawca powinien dostarczyć najpóźniej w dniu podpisania protokołu odbioru przedmiotu zamówienia.
14. Okres gwarancji lub rękojmi ulega odpowiedniemu przedłużeniu o czas, w ciągu którego, wskutek wady przedmiotu umowy objętego gwarancją, Zamawiający nie mógł z niego korzystać.
15. Wykonawca do oprogramowania dostarczonego Zamawiającemu na podstawie umowy dołącza Licencje oraz wszelkie inne dokumenty konieczne do prawidłowego korzystania z Systemu.

16. Dla oprogramowania wymaga się dostarczenia wsparcia technicznego producentów tego oprogramowania na okres minimum 12 miesięcy z możliwością jego odnawiania po tym czasie.

§ 9

W celu zapewnienia skutecznej ochrony oraz zachowania w tajemnicy wszelkich informacji i danych otrzymanych i uzyskanych od Zamawiającemu w związku z wykonaniem zobowiązań wynikających z umowy Wykonawca zobowiązuje się do podpisania umowy o zachowaniu poufności stanowiącej **załącznik nr 3** do umowy wraz załącznikami.
Zobowiązanie to nie jest ograniczone w czasie i wiąże Wykonawcę również po wykonaniu przedmiotu umowy lub jej rozwiązaniu/wygaśnięciu (bez względu na przyczynę) bez prawa do dodatkowego wynagrodzenia z tego tytułu.

§ 10

1. Zamawiający naliczy Wykonawcy karę umowną za niedotrzymanie terminu realizacji umowy, określonego w § 1 ust. 3, w wysokości 0,1 % wynagrodzenia brutto, określonego w § 5 ust. 1 za każdy rozpoczęty dzień zwłoki.
2. Zamawiający naliczy Wykonawcy karę umowną za zwłokę w usunięciu wad/awarii systemu stwierdzonych przy odbiorze lub w okresie gwarancji, w wysokości 0,5 % wynagrodzenia brutto, określonego w § 5 ust. 1 za każdy rozpoczęty dzień zwłoki w stosunku do terminu określonego w § 8 ust.4 pkt 2.
3. W przypadku, gdy zwłoka w realizacji przedmiotu umowy w zakresie określonym w §1 ust. 3 przekroczy 8 dni, Zamawiający ma prawo odstąpić od umowy w niezrealizowanym zakresie, a Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 15 % wynagrodzenia brutto, określonego w § 5 ust. 1 niniejszej umowy.
4. Zamawiający może odstąpić od umowy w niezrealizowanym zakresie w terminie 3 dni roboczych od dnia wskazanego w wezwaniu do realizacji przedmiotu umowy, o którym mowa poniżej, w przypadku nieprzestrzegania przez Wykonawcę któregokolwiek z warunków niniejszej umowy, przy czym odstąpienie od umowy musi być poprzedzone wezwaniem Wykonawcy do realizacji przedmiotu umowy w terminie 3 dni od dnia doręczenia wezwania, zgodnie z opisem przedmiotu zamówienia oraz postanowieniami umowy.
5. Zamawiający naliczy Wykonawcy karę umowną z tytułu odstąpienia od umowy lub wypowiedzenia umowy z przyczyn leżących po stronie Wykonawcy w wysokości 10 % wynagrodzenia brutto, określonego w § 5 ust. 1 niniejszej umowy.
6. Zamawiający zastrzega sobie prawo dochodzenia odszkodowania przewyższającego wartość zastrzeżonych kar umownych, na zasadach ogólnych.
7. Wykonawca wyraża zgodę na potrącenie ewentualnych kar umownych z wynagrodzenia przysługującego za wykonanie przedmiotu umowy.
8. Zamawiający może odstąpić od nałożenia kary lub ją obniżyć, jeżeli Wykonawca wykaże, że opóźnienie nastąpiło z przyczyn całkowicie od niego niezależnych, których nie mógł przewidzieć i którym nie mógł zapobiec.
9. Zapłata przez Wykonawcę kar umownych z tytułu niewykonania lub nienależytego wykonania umowy, nie wyłącza prawa Zamawiającego do dochodzenia odszkodowania przewyższającego ustalone kary umowne na zasadach ogólnych, przy czym odpowiedzialność Wykonawcy z tytułu kar umownych ograniczona jest do 100% wartości umowy brutto, o której mowa w § 5 ust. 1 umowy.

§ 11

Wprowadzenie zmian treści umowy wymaga zgody Stron i sporządzenia pod rygorem nieważności pisemnego aneksu.

§ 12

1. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz.U. 2019 r. poz.1843) oraz ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (t.j. Dz. U. z 2019 r., poz. 1145 ze zm.)
2. Ewentualne sprawy sporne wynikłe w związku z realizacją niniejszej umowy, strony zobowiązują się w pierwszej kolejności załatwić polubownie, a w przypadku niemożności ich polubownego załatwienia, strony mogą poddać je rozstrzygnięciu Sądu właściwego dla siedziby Zamawiającego.
3. Prawa i obowiązki wynikające z niniejszej umowy, mogą być przeniesione na rzecz osób trzecich, wyłącznie za pisemną zgodą Stron.
4. Strony umowy zobowiązują się informować wzajemnie o wszelkich zmianach swoich adresów do doręczeń pod rygorem tego, że wszelkie oświadczenia woli i wiedzy składane sobie w związku z realizacją umowy wysyłane będą na adresy Stron wskazane w komparycji umowy, ze skutkiem ich prawidłowego doręczenia.
5. Wykonawca ma świadomość, że umowa i dane go identyfikujące podlegają udostępnieniu na podstawie informacji o dostępie do informacji publicznej i stanowią informację publiczną w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. 2019, poz. 1429).

§ 13

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, jeden dla Zamawiającego, jeden dla Wykonawcy.

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 1 do projektu umowy

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja oprogramowania służącego do ochrony przed wyciekiem danych wskutek ich kradzieży lub niezamierzonych (nieświadomych) działań użytkowników. Dane te mogą zawierać informacje, które podlegają ochronie z powodów biznesowych (tajemnica przedsiębiorstwa) lub prawnych (osobowe, dane wrażliwe, finansowe, itp.).
W skład oprogramowania będącego przedmiotem zamówienia muszą wchodzić następujące moduły:

- Moduł Data Loss Prevention (zwany dalej DLP).
- Moduł Kontroli Urządzeń (zwany dalej KU).
- Moduł szyfrowania dysków dla systemu Windows (zwany dalej SD).
- Moduł Szyfrowania Plików i Folderów (zwany dalej SP).
- Centralna Konsola Zarządzania (zwana dalej CKZ).

Wymagania ogólne:

1. Dostarczone rozwiązanie powinno być skalowalne i musi być w stanie zarządzać infrastrukturą złożoną z minimum 350 stacji końcowych.
2. Wszystkie komponenty instalowane na stacji roboczej powinny pochodzić od jednego producenta i być zarządzane przez pojedynczą Centralną Konsolę Zarządzania. Centralna Konsola Zarządzania powinna być dostępna jako oprogramowanie instalowane w środowisku wirtualnym Zamawiającego zbudowanym w oparciu o VMware vSphere 6.5.
3. Wszystkimi komponentami po stronie stacji roboczej powinien zarządzać jeden agent, którego zadaniem będzie przekazywanie polityk z CKZ do stacji roboczych oraz przekazywanie zdarzeń z komponentów zarządzanych do CKZ.

Wymagania szczegółowe dla systemu będącego przedmiotem zamówienia:

1. Wszystkie moduły powinny pracować na stacjach klienckich z następującymi systemami operacyjnymi:
   a. Windows 10 (wersja x32 i x64)
   b. Mac OS X 10.10.x, 10.11.x, 10.12.x oraz 10.13.x
2. Moduł KU oraz moduł DLP powinien pracować na następujących systemach serwerowych:
   a. Windows 2012 / 2012 R2 oraz nowszych
3. W przypadku systemów Mac OS oraz Windows Server - Zamawiający dopuszcza pewne różnice we wspieranych funkcjonalnościach w stosunku do systemów Windows.
4. Instalacja systemu będącego przedmiotem zamówienia (co najmniej agenta zarządzającego) powinna być możliwa poprzez instalację ręczną oraz instalację automatyczną z użyciem CKZ lub zewnętrznego oprogramowania do zdalnej instalacji wymagającego plików MSI.
5. Oprogramowanie powinno umożliwić prace w środowiskach całkowicie izolowanych, gdzie nie ma dostępu do Internetu. Powinna istnieć możliwość ręcznej aktualizacji wszystkich komponentów z użyciem CKZ.
6. Graficzny interfejs wszystkich komponentów powinien być dostępny co najmniej w języku angielskim oraz polskim. Powinna istnieć możliwość automatycznego wyboru języka, wyświetlana w zależności od języka klienckiego systemu operacyjnego.
7. W ramach modułów systemu będącego przedmiotem zamówienia powinny być obecne mechanizmy samoobrony przed próbami zatrzymania lub wyłączenia ochrony poprzez te moduły. Powinny być zaimplementowane mechanizmy zapobiegające modyfikacjom zarówno struktury plików, procesów jak i rejestrów niezbędnych do pracy ww. systemu.

Wymagania dotyczące modułu ochrony przed wyciekiem danych (DLP)

KLASYFIKACJA

1. Moduł powinien być odpowiedzialny za odpowiednią klasyfikację plików oraz wymuszanie ochrony zaklasyfikowanych plików poprzez wspierane kanały wycieku danych.
2. Moduł DLP powinien przeprowadzać klasyfikację plików na następujące sposoby:
   a. Klasyfikacja w oparciu o etykiety.
   b. Klasyfikacja w oparciu o typ/zawartość pliku.
   c. Klasyfikacja ręczna dokonana przez użytkownika.

3. 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. Automatyczne nadawanie etykiet w oparciu o aplikację webową z której został wygenerowany (ściągnięty) dany plik.
   d. Ręczne nadawanie etykiet przed administratora systemu lub udziału sieciowego.

4. Klasyfikacja w oparciu o etykiety powinna mieć mechanizm chroniący przed zgubieniem etykiet w wyniku wykonania manipulacji związanych z 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 manualnego przepisania odpowiednio długiego fragmentu pliku do innego dokumentu (bez użycia schowka).

5. Nadanie etykiety w ramach klasyfikacji opartej o etykiety nie może modyfikować zawartości pliku. Uruchomienie funkcji skrótu (jak MD5, SHA1, SHA-256) na pliku przed klasyfikacją i po klasyfikacji powinna dać taki sam wynik.

6. Klasyfikacja w oparciu o typ/zawartość pliku powinna być nadawana w oparciu o następujące parametry:
   a. Słowa kluczowe występujące w pliku. Powinna być możliwość zdefiniowania ile słów kluczowych musi wystąpić by uznać plik za sklasyfikowany. 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 z 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.
f. Atrybuty pliku jeśli jest to dokument pakietu Microsoft Office lub PDF jak co najmniej Autor, Firma, Słowa Kluczowe czy Komentarz.

7. Klasyfikacja danych w oparciu o typ/zawartość powinna być wykonywana dynamicznie przez moduł DLP na stacjach w momencie dostępu do pliku, bez konieczności wykonywania okresowego, masowego znakowania danych.

8. Klasyfikacja ręczna powinna być nadawana przez użytkownika systemu na pliki pakietu Microsoft Office, pliki PDF oraz wysyłaną pocztę w następujących sytuacjach:

   a. Użytkownik zapisuje plik na dysku
   b. Użytkownik próbuje wysłać email poza organizację
   c. Użytkownik wybierze odpowiednią opcję w programach pakietu Microsoft Office.

9. Klasyfikacja ręczna dokonana przez użytkownika powinna w momencie wysyłania email dodać stosowny nagłówek i stopkę w treści maila informujące o poziomie klasyfikacji danego emaila.
10. Nazwy etykiet klasyfikacji danych, zarówno dotyczących klasyfikacji w oparciu o typ/zawartość jak i klasyfikacji w oparciu o etykiety powinny być konfigurowalne przez administratora.

OCHRONA PRZED WYCIEKIEM

1. System powinien chronić dane przed wyciekiem za pomocą następujących kanałów danych:
   a. Ochrona przed wyciekiem przez wydruk
      i. Definiowanie ograniczeń w drukowaniu wskazanych dokumentów sklasyfikowanych, w tym możliwość wskazania, który dokument może być drukowany na której drukarce lokalnej lub sieciowej.
      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, IP adres komputera użytkownika, czas zdarzenia oraz zawartość drukowanego pliku.
   b. Ochrona przed wyciekiem do sieci WEB.
      i. Definiowanie ograniczeń przy wysyłaniu plików sklasyfikowanych z użyciem przeglądarek webowych do Internetu, 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 oraz zawartość wysyłanego pliku.
      iii. Powinny być wspierane co najmniej przeglądarki: Internet Explorer, Edge, Firefox oraz Chrome.
      iv. Blokowanie powinno być również wspierane dla połączeń szyfrowanych przy czym nie dopuszcza się deszyfracji ruchu pomiędzy przeglądarką internetową a serwerem docelowym.
   c. Ochrona przed wyciekiem przez EMAIL
      i. Definiowanie ograniczeń przy wysyłaniu plików sklasyfikowanych z użyciem klientów pocztowych 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 oraz zawartość plików sklasyfikowanych załączonych do wiadomości.
iii. Etykiety klasyfikacji plików dołączanych do email powinny być przekazywane przez email poprzez nadawanie nagłówków do wiadomości lub w inny, podobny sposób tak, by w momencie zapisywania plików na innej stacji roboczej odpowiednia klasyfikacja była automatycznie nadawana.
iv. Klasyfikacja powinna odbywać się po naciśnięciu przycisku „wyślij", jednak przed faktyczną próbą wysłania wiadomości. Po blokadzie wysyłki edytowana wiadomość powinna pozostać otwarta.

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 ekranu oraz sam zrzut ekranu w postaci pliku graficznego.
iii. Powinny istnieć wbudowane definicje programów używanych do zrzutów ekranu i powinna istnieć możliwość dodania własnych definicji. W momencie uruchomienia programu z listy możliwość robienia zrzutów ekranu nie powinna być możliwa.

e. Ochrona przed skopiowaniem plików na zewnętrzne nośniki danych.
i. Definiowanie ograniczeń przy kopiowaniu sklasyfikowanych plików na zewnętrzne dyski oraz kopiowania danych z nośników wymiennych na stacje roboczą.
ii. Monitorowanie, blokowanie kopiowania oraz raportowanie takiego zdarzenia obejmującego minimum nazwę pliku kopiowanego, numer seryjny nośnika zewnętrznego oraz zawartość kopiowanych plików.

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 oraz treść schowka.

g. Ochrona przed wysyłką danych poprzez sieć.
i. Definiowanie ograniczeń przy dostępnie 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 w zakresie minimum nazwy procesu, źródłowego adresu IP, docelowego adresu IP, portu źródłowego, portu docelowego oraz kierunku ruchu.

2. Dostępność różnych rodzajów reakcji modułu DLP na wykryte naruszenia polityki ochrony:
a. Blokowanie akcji (np. blokada wysyłki email ze sklasyfikowanymi załącznikami).
b. Monitorowania akcji (wysłanie incydentu do CKZ).
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 w CKZ.

e. Automatyczne szyfrowanie chronionych plików podczas ich przesyłania do katalogów sieciowych lub na dysk zewnętrzny USB - przy czym administrator systemu ma możliwość wskazania jaki klucz zostanie użyty do szyfrowania i jakie osoby/grupy użytkowników mają prawo dostępu do klucza i zaszyfrowanych danych.
f. Zachowanie dowodów w postaci skopiowania danych, które spowodowały podjęcie akcji przez moduł DLP we wskazanym udziale sieciowym (w tym też obrazy wykonanych zrzutów z ekranu). Dane kopiowane na udział muszą być szyfrowane, a dostęp do nich możliwy tylko z konsoli systemu zarządzania.

3. System powinien dawać możliwość aplikowania różnych reakcji w zależności od tego, czy system znajduje się w sieci korporacyjnej czy poza nią (w szczególności stanowiska mobilne). Badanie obecności w sieci korporacyjnej powinno odbywać się poprzez badanie otwartości dowolnie wybranego portu na dowolnie wybranym serwerze.
4. 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.
   b. Przydzielenie do pliku polityki RM (Rights Management).
   c. Przydzielenie do pliku etykiety klasyfikacji.
   d. Przeniesienie pliku do lokalnej kwarantanny.
      i. Plik w kwarantannie musi być chroniony przed niepowołanym dostępem przez jego zaszyfrowanie.
      ii. Musi być możliwe odzyskanie pliku z kwarantanny przez użytkownika po potwierdzeniu tego przez administratora systemu DLP (proces challenge - response). Przy czym wykonanie odzyskania pliku z kwarantanny nie może wymagać podłączenia stacji do sieci firmowej.
   e. Automatyczne szyfrowanie plików przy czym administrator systemu ma możliwość wskazania jaki klucz zostanie użyty do szyfrowania i jakie osoby/grupy użytkowników mają prawo dostępu do klucza i zaszyfrowanych danych.

5. Musi istnieć możliwość definiowania harmonogramu skanowania okresowego w celu przeszukiwania dysków twardych.

ZADZĄDZANIE INCYDENTAMI

1. System musi znakować czasowo wszystkie zdarzenia napływające do serwera CKZ.
2. Wszystkie incydenty związane z naruszeniem danych powinny mieć nadany priorytet w co najmniej pięciostopniowej skali tak, by możliwe było odróżnienie incydentów bardziej istotnych od mniej istotnych.
3. Powinna istnieć możliwość automatycznego przydzielania incydentów do konkretnego właściciela lub grupy właścicieli oraz informowania przez email nowych właścicieli incydentów.
4. Każdy incydent powinien posiadać odpowiedni status - co najmniej „nowy”, „przejrzany”, „eskalowany”, „rozwiązany” oraz „fałszywy alarm”. System powinien dawać możliwość tworzenia nowych statusów o własnych nazwach.
5. Powinna istnieć możliwość anonimizacji niektórych danych, które jednoznacznie identyfikują użytkownika dla wybranych grup użytkowników. W szczególności powinno być możliwe stworzenie sposobu zarządzania incydentami, gdzie pierwsza linia wsparcia nie ma dostępu do szczegółowych danych incydentu oraz załączonych dowodów a druga linia wsparcia już taki dostęp posiada.

6. Moduł DLP musi współpracować z systemami RM (rights management), co najmniej Microsoft RMS oraz Seclore FileSecure (IRM).
   a. Moduł DLP musi umożliwiać sprawdzenie, czy plik posiada przydzieloną politykę RM, a jeśli nie, zablokować jego wysłanie na zewnątrz.
   b. Moduł DLP musi umożliwiać automatyczne przydzielenie określonej polityki RM do plików podlegających ochronie znajdujących się na dysku stacji użytkownika.

INNE WYMAGANIA

1. System DLP po stronie klienta powinien posiadać polski interfejs użytkownika. Cała komunikacja z użytkownikiem powinna być prowadzona w języku polskim.
2. System powinien wymuszać politykę DLP nawet w sytuacji, gdy zostanie uruchomiony w trybie awaryjnym (tzw. Safe Mode).
3. System DLP powinien umożliwiać czasowe wyłączenie ochrony na stacji klienckiej poprzez mechanizm challange-response. Wyłączenie funkcjonalności powinno być terminowe – na zadany okres czasu od 5 min do 30 dni.
4. System powinien współpracować z sieciowym DLP tego samego producenta. Powinien istnieć pojedynczy punkt konfiguracji hostowego oraz sieciowego systemu DLP.

Wymagania dotyczące modułu Kontroli Urządzeń (KU)

1. Moduł KU musi zapewnić ochronę przed podłączaniem niepożądanych urządzeń do stacji klienckich i powinien być zarządzany przez CKZ.
2. Musi istnieć możliwość skonfigurowania modułu tak, aby jego praca była niewidoczna dla użytkownika (tryb ukryty).
3. Musi istnieć możliwość podania w języku polskim treści informacji o powodzie podjęcia akcji przez moduł KU, która jest wyświetlana użytkownikowi.
4. Moduł musi mieć możliwość: logowania zdarzenia, powiadomienia użytkownika poprzez monit w języku polskim, zablokowania zdarzenia oraz kopiowania przedmiotu akcji (jeśli istnieje) w celach dowodowych na wskazany udział sieciowy (CIFS).
5. Moduł KU musi wykrywać i blokować urządzenia podłączane przez porty zewnętrzne komputera (wliczając w to: USB, Serial, Fire-Wire, Bluetooth), takie jak pendrive, PDA, kamera cyfrowa, odtwarzacze MP3, drukarki i inne typy urządzeń oraz umożliwiać zmianę sposobu dostępu do urządzeń posiadających system plików (pendrive USB, CD/DVD) na tryb „tylko do odczytu”.
6. Rozwiązanie musi przechowywać informacje 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).
7. System powinien umożliwić blokowanie dowolnego urządzenia oraz tworzyć definicje, gdzie blokowane będą wszystkie urządzenia danego typu oprócz wyjątków dodanych przez administratora (na przykład: blokuj wszystkie lokalne drukarki oprócz drukarek o podanych numerach seryjnych).
8. Konfiguracja polityki działania modułu musi umożliwiać zdefiniowanie dopuszczonych do użytkowania nośników danych USB na podstawie ich numeru seryjnego, ID producenta i ID produktu.
9. Polityka działania modułu może być różna (np. bardziej restrykcyjna), jeśli stacja działa poza wewnętrzną, firmową siecią Zamawiającego. Badanie obecności w sieci korporacyjnej powinno odbywać się poprzez badanie otwartości dowolnie wybranego portu na dowolnie wybranym serwerze.
10. Polityka działania modułu musi umożliwiać przypisanie różnych polityk zależnie od przynależności użytkownika do grup użytkowników synchronizowanych z Active Directory.

11. Polityka działania modułu ma umożliwiać zdefiniowanie zawartości plików (na podstawie słów kluczowych oraz wyrażeń regularnych), której wykrycie spowodowuje zablokowanie zapisu pliku na nośnik zewnętrzny, nawet, jeśli został on dopuszczony do użytkowania. W ramach reakcji na incydent powinna istnieć możliwość zapisania pliku wraz z incydentem, którego dotyczyło zablokowane, kopiowanie.
12. System powinien pozwalać nadać każdemu z incydentów właściciela, a każdy administrator powinien mieć ściśle zdefiniowane uprawnienia w ramach separacji obowiązków.
13. System KU powinien umożliwiać czasowe wyłączenie ochrony na stacji klienckiej poprzez mechanizm challange-response. Wyłączenie funkcjonalności powinno być terminowe - na zadany okres czasu od 5 min do 30 dni.

Wymagania dotyczące modułu szyfrowania dysków dla systemu Windows (moduł SD)

1. Rozwiązanie musi zapewnić szyfrowanie danych na poziomie dysku w sposób transparentny dla systemu operacyjnego i użytkownika, z funkcjonalnością uwierzytelniania użytkownika bezpośrednio po uruchomieniu komputera (przed wystartowaniem właściwego systemu operacyjnego - tzw. pre-boot authentication, zwany dalej PBA).
2. System szyfrowania musi zapewniać centralne zarządzanie poprzez CKZ, 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.
3. Oprogramowanie szyfrujące na stacjach użytkowników musi komunikować się z CKZ w bezpieczny sposób (transmisja szyfrowana z obustronną autentykacją) z wykorzystaniem protokołów opartych na TCP/IP, które umożliwiają połączenie przez sieci routowane.
4. Musi istnieć możliwość określenia czy szyfrowaniu mają podlegać wszystkie partycje dysku, czy tylko partycja bootowalna (z której startuje właściwy system operacyjny) czy tylko partycje „niebootowalne". Musi też istnieć możliwość określenie dowolnej konfiguracji partycji do zaszyfrowania.
5. Rozwiązanie musi obsługiwać co najmniej algorytm AES 256 jako algorytm szyfrowania danych. Rozwiązanie musi samodzielnie wykrywać czy procesor chronionego komputera obsługuje sprzętowe wsparcie szyfrowania (Intel AES-NI) i automatycznie wykorzystywać tę funkcjonalność podczas szyfrowania/deszyfrowania danych.
6. Uwierzytelnianie użytkownika w PBA ma być możliwa z wykorzystaniem hasła i nazwy użytkownika, ale także z użyciem kart inteligentnych różnych producentów oraz biometrii.
7. System powinien pozwalać na użycie modułu TPM 2.0 w celu uniknięcia potrzeby ręcznego wpisywania hasła przez użytkowników.
8. Musi być zapewniona obsługa uwierzytelniania użytkowników w trybie PBA z wykorzystaniem systemu PKI (kart inteligentnych przechowujących certyfikaty użytkowników). Wymagana jest obsługa co najmniej Microsoft PKI.
9. System powinien pobierać użytkowników z 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. System musi umożliwiać przypisanie co najmniej 2000 użytkowników (użytkowników lub grup z AD obejmujących w sumie 2000 użytkowników) do jednego komputera.
   b. Użytkownicy i grupy użytkowników przypisywani do komputerów muszą być synchronizowani z domeny Microsoft AD.
   c. Usunięcie użytkownika w serwerze usług katalogowych AD powinno skutkować automatycznym usunięciem lub zablokowaniem użytkownika w serwerze zarządzającym systemem szyfrowania.

   d. System musi umożliwiać automatyczne dodanie do listy uprawnionych użytkowników, użytkowników z domeny AD, którzy wcześniej korzystali z komputera (logowali się do niego).

10. Zmiany hasła użytkownika na jednej maszynie muszą być automatycznie powielane i synchronizowane na pozostałych komputerach, do których jest przypisany ten użytkownik.

11. Zmiana hasła z poziomu systemu Windows powinna być automatycznie replikowana do systemu szyfrującego tak, by nie było potrzeby dwukrotnej zmiany hasła.

12. Rozwiązanie musi umożliwiać pracę w trybie single sign-on - 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.

13. System szyfrowania musi umożliwiać centralną kontrolę jakości haseł używanych przez użytkowników przez określenie minimum: długości hasła, zawartości hasła (znaki numeryczne i alfanumeryczne, symbole, itp.), historię stosowanych haseł, wymuszenie zmiany hasła przez użytkownika.

14. System musi zapewnić centralne przechowywanie kluczy użytych do szyfrowania danych i możliwość odzyskania zaszyfrowanych danych z ich wykorzystaniem w sytuacji awarii.

15. Każdy komputer musi posiadać swój unikalny klucz wykorzystywany do szyfrowania danych na dysku oraz powinien być obecny w bazie CKZ.

16. Oprogramowanie szyfrujące musi kontynuować pracę po niespodziewanym zaniku zasilania, bez wpływu na możliwość zaszyfrowania i odszyfrowania danych.

17. System musi zapewniać możliwość centralnej konfiguracji parametrów szyfrowania, w tym centralne ustalanie polityk dla użytkowników i komputerów.

18. Rozwiązanie powinno umożliwiać definiowanie uprawnień i ról dla kont administratorów.

19. Stacje i użytkownicy mają synchronizować zmiany w politykach szyfrowania i parametrach systemu bez konieczności interwencji administratora.

20. Instalacja oprogramowania szyfrującego na stacjach użytkowników powinna się odbywać z wykorzystaniem paczki instalacyjnej, niezależnej od wersji i rodzaju systemu operacyjnego, zawierającego niezbędne moduły systemu szyfrowania.

21. Instalacja oprogramowania na stacji powinna się odbywać bez interwencji użytkownika.

22. System przed rozpoczęciem szyfrowania powinien sprawdzić, czy na komputerze nie znajduje się oprogramowanie niekompatybilne.

23. System musi umożliwiać zalogowanie się do głównego systemu operacyjnego z pominięciem PBA pod warunkiem wyrażenia na to zgody przez administratora systemu (np. celem zdalnej instalacji oprogramowania na stacji, bez obecności ich użytkownika) bez obecności modułu TPM. Pominięcie PBA musi być możliwe w z góry określonym przedziale czasu i na żądanie z poziomu stacji pod warunkiem, że używane jest do tego konto administratora domeny i pod warunkiem, że taki tryb pominięcia PBA jest zgodny z centralnie określoną polityką.

24. System powinien 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.

25. Musi istnieć dobrze zdefiniowany proces odzyskiwania danych w sytuacjach awaryjnych: zagubienie hasła i nazwy użytkownika, po uszkodzeniu systemu operacyjnego, po uszkodzeniu systemu szyfrowania.

   a. Obsługa mechanizmu resetowania/odzyskiwania hasła użytkownika w rozwiązaniu do szyfrowania danych nie może wymagać podłączenia stacji do sieci firmowej.

b. Musi istnieć możliwość samodzielnego zresetowania hasła przez użytkownika w trybie PBA w oparciu o udzielenie odpowiedzi na wcześniej zdefiniowane pytania, bez konieczności podłączenia stacji do sieci firmowej.
c. Musi istnieć możliwość odzyskiwania dostępu do danych przy pomocy aplikacji dla smartfona użytkownika. Aplikacja do obsługi tego odzyskiwania powinna być dostępna bezpłatnie minimum dla systemu Android.
d. W sytuacji zablokowania lub usunięcia oprogramowania szyfrującego zainstalowanego na stacji użytkownika musi być dostępny mechanizm i narzędzie do odzyskania zaszyfrowanych danych oraz odinstalowania oprogramowania szyfrującego opartego na narzędziu typu liveCD.

26. System szyfrowania dysków musi obsługiwać dyski twarde z wbudowanym mechanizmem szyfrowania sprzętowej w standardzie OPAL.
a. Po automatycznym wykryciu takiego dysku, oferowane rozwiązanie musi przekazać obsługę szyfrowania do wbudowanego mechanizmu w dysku.
b. Rozwiązanie musi być przetestowane przez producenta z minimum czteroma różnymi dyskami OPAL. Producent powinien zapewnić dostęp do listy kompatybilności dysków z OPAL.

27. System musi oferować możliwość wykorzystania wbudowanego mechanizmu szyfrowania w system operacyjny zamiast własnego mechanizmu szyfrującego. Wtedy system będzie odpowiedzialny za konfigurację funkcjonalności Bitlocker w przypadku systemów Microsoft Windows oraz FileVault w przypadku systemów Mac OS.

Wymagania dotyczące modułu szyfrowania plików i folderów (moduł SP)

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 urządzenia zewnętrzne USB oraz CD/DVD.
c. zabezpieczenie danych przenoszonych na USB między komputerami poprzez utworzony na dysku USB szyfrowany kontener.
d. integrację z podsystemem ochrony przed wyciekiem danych DLP opisanym powyżej, co najmniej poprzez wymuszenie sterowania szyfrowania plików kopiowanych na nośniki USB z poziomu polityki DLP.

2. System szyfrowania plików i folderów musi być możliwy do wdrożenia niezależnie od modułu szyfrowania danych (SD).
3. Moduł SP powinien mieć w pełni spolonizowany interfejs użytkownika.
4. Instalacja oprogramowania na stacjach użytkowników powinna się odbywać z wykorzystaniem paczki instalacyjnej, niezależnej od wersji i rodzaju systemu operacyjnego, zawierającej niezbędne moduły i opcjonalnie parametry polityki szyfrowania.
5. Instalacja oprogramowania na stacji powinna się odbywać bez interwencji użytkownika.
6. System szyfrowania SP musi zapewniać centralne zarządzanie, w oparciu o CKZ.
7. Oprogramowanie szyfrujące na stacjach użytkowników musi komunikować się z serwerem zarządzającym w bezpieczny (transmisja szyfrowana z obustronną autentykacją) sposób z wykorzystaniem protokołów opartych na TCP/IP.
8. Rozwiązanie musi wykorzystywać algorytm AES 256 do szyfrowania danych.
9. Szyfrowanie plików nie powinno wpływać na datę ostatniego dostępu do pliku zapisanej w atrybutach pliku.

10. Powinien istnieć mechanizm ograniczający utylizację dysku twardego do zadanej wartości procentowej przy szyfrowaniu plików tak, by samo szyfrowanie nie wpływało na komfort pracy użytkownika.
11. Oprogramowanie SP powinno umożliwić stworzenie listy wyjątków przy dostępie do plików zaszyfrowanych tak, by ich praca nie była wstrzymywana w przypadku próby dostępu do pliku zaszyfrowanego kluczem, do którego użytkownik nie ma dostępu (np. dla systemu antywirusowego lub backupowego).
12. System powinien wspierać wymazywanie zawartości pliku z dysku przy kasowaniu pliku tak, by niemożliwe było jego odzyskanie.
13. System powinien umożliwić tworzenie kluczy synchronizowanych z CKZ oraz takich generowanych lokalnie - nie podlegających synchronizacji z CKZ. Klucze lokalne powinny być tworzone bezpośrednio przez użytkowników.
14. Możliwość tworzenia kluczy nie podlegających synchronizacji z CKZ powinna być możliwa do zablokowania.
15. Tworzenie i przechowywanie kluczy powinno odbywać się na CKZ. Wszystkie klucze za wyjątkiem kluczy zdefiniowanych lokalnie powinny być przechowywane w bazie CKZ powinno być możliwe ich odzyskanie w sytuacji awaryjnej.
16. System musi zapewniać centralne przydzielenie tych samych kluczy używanych do szyfrowania do wielu użytkowników i grup użytkowników z Active Directory (AD).
17. Niezależnie od centralnie przydzielonych wspólnych kluczy dla grupy użytkowników, każdy użytkownik musi posiadać także unikalny klucz, przypisany do niego automatycznie, wykorzystywany do szyfrowania plików i katalogów.
18. Musi istnieć możliwość użycia kluczy wykorzystywanych do szyfrowania plików i katalogów oraz USB/CD/DVD także w trybie off-line (kiedy stacja nie jest podłączona do sieci Zamawiającego i jeśli nie ma połączenia z centralnym serwerem zarządzającym).
19. Decyzja o zaszyfrowaniu pliku może zostać podjęta w oparciu o:
  a. Centralnie zdefiniowaną politykę wskazująca foldery/pliki obligatoryjnie szyfrowane ze wskazaniem konkretnego klucza szyfrującego.
  b. Lokalnie przez użytkownika z użyciem kluczy, do których użycia użytkownik jest uprawniony.
20. W przypadku centralnie definiowanej polityki powinno być możliwe, co najmniej:
  a. Wskazanie plików/folderów, które powinny być obligatoryjnie szyfrowane.
  b. Wskazanie udziałów sieciowych, których pliki powinny być zaszyfrowane. Szyfrowanie udziałów sieciowych nie może wymagać instalowania oprogramowania na serwerach plików. Komunikacja między stacją użytkownika a udziałem sieciowym z zaszyfrowanymi plikami nie może powodować, że pliki lub ich części są przesyłane niezaszyfrowane.
  c. Wskazanie usług chmurowych (co najmniej: Box, Dropbox, Googe Drive, Microsoft Onedrive), których pliki będą szyfrowane przed synchronizacją.
  d. Przy wskazywaniu plików/folderów powinna istnieć możliwość użycia typowych, predefiniowanych lokalizacji jak pulpit systemowy, katalog profilu użytkownika, itp.
  e. Określenie typów plików, jakie mają być szyfrowane przez wskazanie procesu jakie je tworzy i rozszerzeń plików.
21. W przypadku ręcznego szyfrowania przez użytkownika powinno być możliwe co najmniej:
  a. Ręczne zaszyfrowanie pliku/katalogu wybranego przez użytkownika wybranym kluczem do którego użytkownik ma dostęp.
  b. Stworzenia samo-rozpakowującego się, zaszyfrowanego archiwum chronionego hasłem wybranym przez użytkownika

c. Użycia funkcji „zaszyfruj i wyślij mailem”, która tworzy nową wiadomość z załączonym zaszyfrowanym plikiem.

22. Pliki zaszyfrowane modułem SP powinny być wizualnie oznaczane zmianą ikony tak, by użytkownik wiedział o stanie zaszyfrowania pliku bez podejmowania dodatkowych akcji.

23. Użytkownik powinien mieć możliwość łatwego sprawdzenia którym kluczem dany plik pozostał zaszyfrowany.

24. Plik zaszyfrowany konkretnym kluczem powinien być automatycznie możliwy do odczytania przez wszystkich użytkowników, którzy mają dostęp do klucza użytego do zaszyfrowania pliku na wszystkich stacjach roboczych.

25. Uwierzytelnianie użytkownika na potrzeby systemu SP musi wykorzystywać uwierzytelnianie Microsoft Windows i umożliwiać przezroczystą pracę dla użytkowników bez potrzeby dodatkowego uwierzytelniania się.

26. W przypadku, gdy zamawiający zrezygnuje z mechanizmów uwierzytelniania wbudowanych w Microsoft Windows powinna istnieć możliwość wykorzystania wbudowanego systemu uwierzytelniania do modułu SP.

27. Uwierzytelnianie użytkownika na potrzeby modułu SP musi umożliwiać użycie tokenów sprzętowych, kart inteligentnych i certyfikatów PKI, które są obsługiwane przez Microsoft Windows.

28. System musi umożliwiać dostęp do danych zaszyfrowanych przez wielu użytkowników (min. 100) zarówno w przypadku szyfrowania plików i katalogów jak również plików szyfrowanych przy kopiowaniu na USB/CD/DVD.

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

30. System SP musi obsługiwać dowolne nośniki wymienne USB i umożliwiać szyfrowanie na nich plików. Powinny istnieć następujące możliwości szyfrowania nośników wymiennych:

a. Szyfrowanie proste, poprzez wymuszenie szyfrowania kopiowanych plików wprost na dysk USB. Pliki nie mogłyby być odczytane na zewnętrznej stacji roboczej nienależącej do organizacji.

b. Szyfrowanie poprzez kontener. Odczytanie plików jest możliwe zarówno na stacjach korporacyjnych jak i zewnętrznych po podaniu hasła ustawionego przy inicjalizacji takiego nośnika.

31. Szyfrowanie poprzez kontener musi spełnić następujące wymagania:

a. Założony katalog musi być dostępny, po podaniu hasła, na innych komputerach bez konieczności instalowania na nich jakiegokolwiek dodatkowego oprogramowania na zewnętrznych stacjach.

b. Kontener musi być gotowy do pracy zaraz po wpięciu pamięci USB do komputera w przypadku stacji korporacyjnej bez konieczności wpisywania hasła.

c. Użytkownik może wybrać podczas inicjalizacji jak duży obszar dysku może zostać zajęty przez kontener. Powinna być możliwość wymuszenia zajęcia całego obszaru dysku przez kontener.

d. Powinna istnieć procedura odzyskiwania dostępu do kontenera poprzez mechanizm challenge/response polegający na wymianie kodów pomiędzy użytkownikiem a operatorem helpdesk.

Wymagania dotyczące Centralnej Konsoli Zarządzająca(CKZ)

Centralna konsola zarządzająca (zwana dalej CKZ) ma za zadanie zarządzanie wszystkimi produktami bezpieczeństwa wchodzącymi w skład rozwiązania będącego przedmiotem niniejszego zamówienia. Powinna się składać z oprogramowania serwerowego oraz agenta instalowanego na stacjach

końcowych, którego zadaniem jest konfigurowanie produktów zarządzanych oraz zbieranie zdarzeń i przekazywanie ich do CKZ.

1. Zarządzanie wszystkimi modułami i pełnym zakresem funkcji dostarczonego systemu ochrony musi następować z jednej i tej samej aplikacji (konsoli) działającej na serwerze Microsoft Windows (wymagane wsparcie dla wersji Windows 2012 R2 oraz Windows 2016) i korzystającej z bazy danych Microsoft SQL (wymagane wsparcie dla wersji SQL 2008, SQL 2008R2, SQL 2012, SQL 2016 – wszystkie w wersji Express i wersjach komercyjnych).
   a. Platforma sprzętowa dla wdrożenia systemu zarządzania, system operacyjny Microsoft Windows oraz serwer Microsoft SQL zostaną zapewnione przez Zamawiającego.
   b. Aplikacja musi być skalowalna i umożliwiać zarządzanie co najmniej 2 tys. komputerów i zainstalowanych na nich produktów.
   c. Wdrożenie dowolnej ilości dodatkowych serwerów zarządzających zarówno pracujących niezależnie od siebie jak również w układzie hierarchicznym nie może wymagać zakupu dodatkowych licencji lub oprogramowania.
   d. System musi umożliwiać migrację zarządzanych komputerów między serwerami zarządzającymi (zmiana przypisania komputera do konkretnego serwera zarządzającego).
   e. System musi umożliwiać odzyskiwanie w przypadku awarii (Disaster Recovery) a konfiguracja potrzebna do odtworzenia serwera powinna być przechowywana w bazie danych.
2. System zarządzający musi mieć możliwość działania w klastrze HA zbudowanym na bazie klastra Microsoft Windows.
3. Centralna konsola zarządzająca ma 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.
   a. Oferowane rozwiązanie powinno umożliwiać metodę dystrybucji oprogramowania poprzez wygenerowanie specjalnego adresu URL, którego dystrybucja dla użytkowników końcowych przez inny kanał komunikacji (np. Email) pozwoli na ściągnięcie i instalacji produktów.
   b. Oferowane rozwiązanie ma umożliwiać selektywne wskazanie, który z produktów ochronnych wchodzących w skład systemu zostanie wdrożony i na którym z komputerów. Nie jest dopuszczalne wdrożenie pakietu w postaci jednej paczki instalacyjnej obejmującej kilka produktów na raz.
   c. Definiowanie komputerów, które mają być objęte wdrożeniem poszczególnych produktów musi być możliwe na bazie zdefiniowanych grup maszyn oraz na bazie dynamicznie przydzielanych znaczników, niezależnie od podziału na grupy maszyn, uzależnionych od parametrów komputera - co najmniej takich jak: rodzaj CPU, ilość RAM, wielkość dysku, rodzaj systemu operacyjnego, ilość dostępnego miejsca na dysku.
4. Zarządzanie powinno odbywać się poprzez standardową przeglądarkę WWW i połączenie https. Nie jest dopuszczalne wykorzystanie do zarządzania dedykowanych aplikacji (tzw. thick client / gruby klient) instalowanych na stacjach administratorów. Powinny być wspierane przeglądarki minimum Internet Explorer 9, Firefox 10 lub Google Chrome 17 oraz Safari 6.
5. Komunikacja wszystkich produktów wdrożonych na danym komputerze musi odbywać się okresowo, w jednolity sposób, poprzez jeden kanał komunikacji inicjowany ze strony chronionych komputerów.
   a. Musi być możliwe wymuszenie połączenia komputera z serwerem zarządzającym na żądanie, ze strony konsoli zarządzania.

b. Muszą istnieć mechanizmy, gdzie jeden z komputerów może być węzłem pośredniczącym dla innych komputerów znajdujących się w tej samej domenie rozgłoszeniowej w przypadku wywołania na żądanie ze strony konsoli zarządzania oraz w przypadku, gdy komputer nie ma bezpośredniego połączenia z serwerem zarządzającym.

c. Komunikacja musi być obustronnie uwierzytelniania z pomocą certyfikatów cyfrowych wygenerowanych dla poszczególnych komponentów komunikujących się poprzez sieć.

6. Centralna aplikacja zarządzająca CKZ musi umożliwiać tworzenie szczegółowych konfiguracji pracy poszczególnych produktów i dystrybucję polityk oraz wymuszanie ich zastosowania.

a. System musi umożliwiać definiowanie dedykowanych wersji polityki działania poszczególnych produktów.

b. System musi umożliwiać przydzielenie różnych polityk działania do poszczególnych komputerów, grup maszyn oraz dynamicznie (niezależnie od przydziału do grupy maszyn) na podstawie filtrów bazujących na parametrach komputerów (co najmniej rodzaj CPU, wielkość RAM, wielkość dysku, ilość wolnego miejsca na dysku, rodzaj systemu operacyjnego).

c. Musi być dostępna funkcjonalność wymuszania, co zdefiniowany przedział czasowy, konfiguracji w przypadku, gdy użytkownik zmieni w niej cokolwiek (pod warunkiem, że zmiana przez użytkownika jest dozwolona w polityce).

d. W przypadku modyfikacji polityki system musi wskazać, ile systemów zostanie dotkniętych zmianą edytowanej polityki.

7. W ramach konsoli powinno być dostępne wersjonowanie polityk produktów zarządzanych. Powinna też być możliwość przywrócenia dowolnej wersji polityki używanej w przeszłości oraz porównania jej z bieżącą polityką.

8. CKZ musi posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP i syslog lub wywołania komendy/skryptu.

9. CKZ musi mieć możliwość integracji z Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i uwierzytelnienia administratorów i dynamicznego przypisywania uprawnień w serwerze zarządzającym w zależności od przynależności do odpowiedniej grupy w Active Directory.

10. System zarządzania CKZ musi być przygotowany 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 z aplikacją zarządzającą nie był narażony na potencjalne ataki z zewnątrz.

11. System zarządzania CKZ ma zapewnić centralne repozytorium (oparte na relacyjnej bazie danych MS SQL) 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 centralnie zarządzanie z pojedynczej konsoli dla wszystkich komponentów oprogramowania.

12. Aplikacja zarządzająca CKZ ma umożliwiać centralne opracowanie raportów na podstawie zgromadzonych danych i prezentację ich w różnych formatach (co najmniej 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.

13. CKZ musi umożliwiać zdefiniowanie wielu kont administratorów i przydzielenie im szczegółowych ról umożliwiających co najmniej: ograniczenie dostępu do wskazanych grup maszyn, ograniczenie administracji do poszczególnych produktów i ich specyficznych funkcji.

14. CKZ musi mieć wbudowane mechanizmy integracji z serwisami zarządzania helpdesk i zgłoszeniami serwisowymi (co najmniej BMC Remedy i HP Service Desk).

15. System powinien posiadać możliwość skanowania w poszukiwaniu niezarządzanych hostów w sieci poprzez instalowanie odpowiedniego oprogramowania na systemy zarządzane. Skanowanie powinno odbywać się przez pasywne nasłuchiwanie ruchu rozgłoszeniowego (np.: ARP, DHCP). Wyniki skanowania powinny być przesyłane do centralnej konsoli w celu dalszej analizy.

16. CKZ musi posiadać dostępny bez dodatkowych opłat 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.

17. Pliki instalacyjne i inne elementy, których dostępność jest wymagana do poprawnej pracy środowiska powinny być zlokalizowane w centralnym repozytorium na konsoli zarządzającej

a. Powinien istnieć mechanizm dystrybucji plików instalacyjnych na zdalne repozytoria danych zapewnione przez zamawiającego obsługujące co najmniej protokoły FTP, HTTP i UNC.

b. Replikacja centralnego repozytorium na repozytoria dodatkowe powinna być możliwa na żądanie oraz powinno być możliwe zdefiniowanie harmonogramu.

c. Powinna istnieć możliwość definicji listy repozytoriów, z których chronione komputery będą korzystały osobno dla różnych grup komputerów. Wybór repozytorium powinien się odbywać zgodnie z kolejnością na liście lub czasów odpowiedzi na ping.

d. W przypadku lokalizacji, gdzie nie ma możliwości skorzystania z serwerów dla zdalnych repozytoriów - taką rolę powinien przejąć dowolny z systemów. System ten powinien mieć możliwość buforowania plików instalacyjnych. Powinna istnieć możliwość tworzenia hierarchii ze wspomnianych wyżej systemów.

Wymagania dotyczące usługi wdrożenia rozwiązania.

1. Wykonanie projektu technicznego, zwanego dalej Projektem Technicznym, oraz przeniesienie autorskich praw majątkowych do Projektu Technicznego, oraz praw zależnych.

2. Dostawa oprogramowania wraz z koniecznymi licencjami na korzystanie z oprogramowania w ilości niezbędnej do budowy i uruchomienia Systemu wraz z 36-miesięcznym wsparciem technicznym producenta oprogramowania (maintenance), zwanego dalej Oprogramowaniem.

3. Wykonanie usług instalacyjno-wdrożeniowych, zgodnie z Projektem Technicznym, w ramach którego zostanie zaimplementowane wdrożenie minimum 5 scenariuszy zapobiegania wyciekowi danych.

4. Prace wdrożeniowe muszą odbywać się w godzinach pracy Zamawiającego, od poniedziałku do piątku w godzinach 8:00 - 16:00.

5. Wykonanie dokumentacji powykonawczej wykonanych usług instalacyjno-wdrożeniowych, zwanej dalej Dokumentacją Powykonawczą, oraz przeniesie autorskich praw majątkowych do Dokumentacji Powykonawczej, oraz praw zależnych.

6. Przeprowadzenie warsztatów instruktażowo-szkoleniowych dla pracowników Zamawiającego z zakresu obsługi wdrożonego Systemu.
7. Świadczenie usługi wsparcia serwisowego Wykonawcy dla Systemu, zwanej dalej Usługą Serwisową.
8. Świadczenie usług konsultacyjnych, w minimalnej ilości 150 godzin w okresie obowiązywania Umowy.

Załącznik nr 2 do projektu umowy

Łódź, dnia …… 2020 r.

PROTOKÓŁ ODBIORU

Zamawiający:
Łódzki Oddział Wojewódzki Narodowego Funduszu Zdrowia
z siedzibą w Łodzi przy ul. Kopcińskiego 58, kod pocztowy 90-032,
będący płatnikiem podatku VAT, NIP 107-000-10-57,
reprezentowany przez:
…….

Wykonawca:
…….
z siedzibą w ……. przy ul. ……..…kod pocztowy……,
będący płatnikiem VAT, NIP: …….., REGON: …….. ,
wpisany do ……...……...
reprezentowany przez:
…….

PRZEDMIOT ODBIORU

Zgodny z postanowieniami umowy nr ……./2019 zawartej w wyniku postępowania o udzielenie zamówienia publicznego nr ZP/ŁOW NFZ/6/2019 prowadzonego w trybie przetargu nieograniczonego na podstawie przepisów ustawy Prawo zamówień publicznych z dnia 29 stycznia 2004 r. (t.j. Dz.U.2019 r. poz. 1843).

Zakres wykonania zamówienia obejmował: ……..……
……
……
……

Uwagi:
……
……
……

Niniejszy protokół stanowi podstawę do wystawienia faktury.

Podpis przedstawiciela Zamawiającego:	**Podpis przedstawiciela Wykonawcy:**
……	……

Załącznik nr 3 do projektu umowy

UMOWA O ZACHOWANIU POUFNOŚCI W NFZ

Zawarta w dniu …… 2019 roku w Łodzi pomiędzy:

Łódzkim Oddziałem Wojewódzkim Narodowego Funduszu Zdrowia
z siedzibą w Łodzi, przy ul. Kopcińskiego 58, kod pocztowy 90-032
będącym płatnikiem podatku VAT, NIP 107-00-01-057
reprezentowanym przez:
……
zwanym dalej **Zamawiającym**,
a
……...……,
z siedzibą w ……...……..,
wpisanym do ……...……,
będącym płatnikiem podatku VAT, NIP: ……, REGON: ..……..……..…….…,
wpisanym do ……..……..……
reprezentowanym przez ……..……
zwanym dalej **Wykonawcą.**

W związku z podpisaniem umowy nr …../2019 z dnia ……. 2019 r., której przedmiotem jest **zakup systemu do ochrony przed wyciekiem danych (DLP)**, zwanej dalej „umową podstawową", strony w celu właściwej ochrony danych poufnych udostępnianych wzajemnie w trakcie realizacji umowy podstawowej postanawiają co następuje:

§ 1.

Ilekroć w umowie użyte zostają wyrazy „Informacje Poufne" oznaczają one:

1) przekazywane Wykonawcy wszelkie informacje lub dane, ustne, na piśmie lub zapisane w inny sposób, dotyczące spraw, planów działalności gospodarczej lub przedsięwzięć strony związanych z realizacją umowy podstawowej,
2) wszelkie rozmowy lub rokowania prowadzone pomiędzy przedstawicielami stron w związku z realizacją umowy oraz informacje przekazywane w ich trakcie przez Zamawiającego.

§ 2.

1. Z uwagi na udostępnianie Informacji Poufnych Wykonawca, zobowiązuje się do:
   1) zachowania w tajemnicy wszystkich Informacji Poufnych, niezależnie od formy w jakiej zostały mu przekazane;
   2) wykorzystywania Informacji Poufnych wyłącznie na użytek prowadzonej współpracy w zakresie realizacji umowy podstawowej;
   3) zapewnienia odpowiedniego i bezpiecznego sposobu przechowywania wszystkich uzyskanych Informacji Poufnych w czasie, gdy znajdują się one w posiadaniu Wykonawcy,
   4) ujawnienia Informacji Poufnych wyłącznie osobom biorącym udział w realizacji umowy podstawowej ze strony Wykonawcy, którym informacje te są niezbędne dla prawidłowej realizacji umowy;

5) poinformowania osób, o których mowa w § 2 ust. 1 pkt 4 umowy, o zachowaniu poufności o poufnym charakterze udostępnianych i przekazywanych informacji, pouczenia w sprawie ich traktowania jako poufnych oraz odebrania oświadczenia wskazanego w § 2 ust. 5 umowy o zachowania poufności;
6) niekopiowania, niepowielania ani niezwielokrotniania Informacji Poufnych w jakikolwiek sposób, chyba że wcześniej w sposób wyraźny udzielona zostanie na taką czynność pisemna zgoda i dokonanie czynności jest obiektywnie niezbędne w związku z realizacją umowy. Zamawiający zobowiązuje się do ujawnienia Informacji Poufnych na potrzeby realizacji umowy osobom biorącym udział w realizacji umowy podstawowej ze strony Wykonawcy, które okażą upoważnienia Zamawiającemu do udziału w realizacji umowy;
7) na pisemny wniosek Zamawiającego lub w przypadku zakończenia współpracy, niezwłocznego zwrócenia lub zniszczenia na własny koszt wszelkich materiałów zawierających jakiekolwiek Informacje Poufne Zamawiającego, wraz ze wszystkimi kopiami, będącymi w jego posiadaniu.

2. W przypadku naruszenia przez Wykonawcę obowiązków dotyczących Informacji Poufnych, o których mowa w niniejszej Umowie, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,1 % wartości całkowitej umowy za każdą ujawnioną Informację Poufną, na żądanie Zamawiającemu, w terminie do 14 dni od chwili ujawnienia.
3. Za przetwarzanie danych osobowych niezgodnie z przepisami prawa ochrony danych osobowych oraz z obowiązkami o których mowa w niniejszej umowie, jak również za jakiekolwiek naruszenia zakresu i celu ich przetwarzania, Wykonawca ponosi wobec Zamawiającego pełną odpowiedzialność.
4. Zamawiający zastrzega sobie prawo do dochodzenia, na zasadach ogólnych, odszkodowania w wysokości przewyższającej karę umowną, w przypadku, gdy szkoda poniesiona przez Stronę poszkodowaną przekracza wysokość kary umownej, o której mowa w ust. 2.
5. Wykonawca oraz osoby biorące udział w realizacji umowy ze strony Wykonawcy złożą oświadczenia zobowiązujące ich do zachowania w tajemnicy Informacji Poufnych, według wzorów określonych w załącznikach do umowy, które Wykonawca niezwłocznie przekaże Zamawiającemu, przed rozpoczęciem wykonywania umowy podstawowej.

§ 3.

1. Zobowiązania określone w § 2 nie mają zastosowania do Informacji Poufnych:
   1) które są w dniu ujawnienia publicznie znane,
   2) których ujawnienie wymagane jest od Wykonawcy na mocy przepisów prawa.
2. Jeżeli Wykonawca zostanie zobowiązany na mocy prawa lub wezwania sądu do ujawnienia jakichkolwiek Informacji Poufnych, niezwłocznie zawiadomi na piśmie Zamawiającego przed dokonaniem ujawnienia.
3. Wykonawca zobowiązany na mocy prawa lub wezwania sądu do ujawnienia Informacji Poufnych, będzie uprawniony do ujawnienia Informacji Poufnej wyłącznie w zakresie wymaganym prawem oraz zobowiązany do podjęcia wszelkich uzasadnionych środków, mających na celu upewnienie się, że Informacje Poufne są traktowane jako poufne.

§ 4.

Wykonawca ponosi odpowiedzialność za przestrzeganie postanowień niniejszej umowy przez swoich pracowników lub inne osoby, które będą zaangażowane w proces realizacji umowy.

§ 5.

Niniejsza Umowa zostaje zawarta na okres obowiązywania umowy podstawowej, z tym że zobowiązanie do zachowania tajemnicy i poufności Informacji Poufnych i odpowiedzialność z tego tytułu, pozostają w mocy także po wygaśnięciu niniejszej Umowy oraz umowy podstawowej.

§ 6.

Wykonawca potwierdza i wyraża zgodę na to, że nie będzie uprawniony do nabycia żadnych praw do Informacji Poufnych przekazanych przez Zamawiającego lub od niego uzyskanych.

§ 7.

1. Strony poddają rozstrzygnięcie sporów powstałych na gruncie niniejszej umowy właściwemu miejscowo ze względu na siedzibę Zamawiającego sądowi powszechnemu.
2. Do wszystkich kwestii nieuregulowanych w niniejszej Umowie znajdują zastosowanie w szczególności przepisy kodeksu cywilnego oraz inne obowiązujące przepisy prawne.

§ 8.

Zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§ 9.

Załącznik do umowy (oświadczenie o zobowiązaniu do zachowania poufności) stanowi integralną część umowy o zachowaniu poufności.

§ 10.

Niniejsza Umowa sporządzona została w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

ZAMAWIAJĄCY:	**WYKONAWCA:**
…….	…….

Załącznik nr 1 do umowy o zachowaniu poufności
(3a)

……
(imię i nazwisko)

OŚWIADCZENIE
o zobowiązaniu do zachowania poufności
dla Wykonawcy / osoby reprezentującej Wykonawcę

Ja niżej podpisany, w związku z realizacją umowy **nr ……/2019** w siedzibie Łódzkiego OW NFZ, z uwagi na udostępnianie Informacji Poufnych, zobowiązuje się do:

1) zachowania w tajemnicy wszystkich Informacji Poufnych uzyskanych podczas realizacji umowy, przedmiotem której jest **zakup systemu do ochrony przed wyciekiem danych (DLP)**, w okresie realizacji zamówienia, a także po wygaśnięciu lub rozwiązaniu umowy, niezależnie od formy w jakiej zostały mi przekazane.
2) wykorzystywania Informacji Poufnych uzyskanych podczas realizacji umowy wyłącznie w celu realizacji umowy.

…… ……
miejscowość, data czytelny podpis

KLAUZULA INFORMACYJNA
DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH
OFERENTÓW I KONTRAHENTÓW WSPÓŁPRACUJĄCYCH
LUB ZAMIERZAJĄCYCH WSPÓŁPRACOWAĆ
Z ŁÓDZKIM ODDZIAŁEM WOJEWÓDZKIM NFZ (3a)

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, dalej: RODO) - Łódzki Oddział Wojewódzki NFZ informuje:

- **ADMINISTRATOR DANYCH OSOBOWYCH**

Narodowy Fundusz Zdrowia, reprezentowany przez Dyrektora Łódzkiego Oddziału Wojewódzkiego NFZ, w zakresie danych osobowych przetwarzanych w Oddziale Wojewódzkim, z którym mogą się Państwo skontaktować w następujący sposób:

- listownie na adres siedziby administratora: ul. Kopcińskiego 58, 90-032 Łódź,
- za pomocą platformy ePUAP
- e-mailem: sekretariat@nfz-lodz.pl.

- **INSPEKTOR OCHRONY DANYCH**

W sprawach dotyczących przetwarzania Państwa danych przez Łódzki Oddział Wojewódzki NFZ można kontaktować się z Inspektorem Ochrony Danych w następujący sposób:

- listownie na adres siedziby administratora: ul. Kopcińskiego 58, 90-032 Łódź**,**
- telefonicznie: (42) 275 40 28,
- e-mailem: IOD@nfz-lodz.pl.

- **CEL I PODSTAWY PRZETWARZANIA**

Państwa dane osobowe będą przetwarzane w celu i związku związanym ze złożoną ofertą / postępowaniem na **zakup systemu do ochrony przed wyciekiem danych (DLP)**, prowadzonym

w trybie **przetargu nieograniczonego** a następnie w związku z ewentualnym zawarciem i realizacją umowy, zleceniem usług lub zamówieniem dostaw oraz ich realizacją.
Podstawą prawną przetwarzania Państwa danych są w szczególności:

- RODO w szczególności art. 6 ust. 1 lit c - w zakresie danych osobowych zawartych w dokumentach wynikających z ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz podlegających archiwizacji na podstawie przepisów prawa;
- RODO, w szczególności art. 6 ust. 1 lit b – w zakresie niezbędnym do zawarcia i realizacji umowy;
- RODO, w szczególności art. 6 ust. 1 lit f – w zakresie niezbędnym do realizacji prawnie uzasadnionego interesu polegającego na weryfikacji i wyborze najkorzystniejszej oferty;
- ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
- ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;
- ustawa z dnia 29 stycznia 2004 r. prawo zamówień publicznych;
- ustawa z dnia 23 kwietnia 1964 r. kodeks cywilny;
- ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych;
- ustawa z dnia 29 września 1994 r. o rachunkowości;
- ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej;
- ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

- **ODBIORCY DANYCH OSOBOWYCH**

Odbiorcami Państwa danych osobowych mogą być podmioty posiadające upoważnienie do pozyskiwania danych osobowych na podstawie przepisów prawa powszechnie obowiązującego (w tym na podstawie ustawy o dostępie do informacji publicznej, ustawy prawo zamówień publicznych oraz ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych). Dane osobowe mogą zostać przekazane podmiotom, z którymi administrator danych osobowych zawarł umowę powierzenia przetwarzania danych osobowych. Administrator danych osobowych nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego, z zastrzeżeniem sytuacji gdy taki obowiązek wynika z przepisu prawa powszechnie obowiązującego.

- **OKRES PRZECHOWYWANIA DANYCH**

Państwa dane osobowe będą przechowywane do chwili realizacji zadania, do którego zostały zebrane oraz przez czas niezbędny do obrony roszczeń, a także przez czas wynikający z przepisów ustawy o narodowym zasobie archiwalnym i archiwach.

- **PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ**

W odniesieniu do danych przetwarzanych we wskazanym celu osobie, której dane dotyczą przysługuje:

- prawo dostępu do treści swoich danych;
- prawo do sprostowania danych;
- prawo do ograniczenia przetwarzania;
- prawo do wniesienia sprzeciwu wobec przetwarzania;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Każde z w/w żądań zostanie indywidualnie rozpatrzone, zgodnie z RODO.

- **INFORMACJA O WYMOGU PODANIA DANYCH**

Podanie przez Państwa danych osobowych jest dobrowolne, jednak niezbędne do rozpatrzenia oferty, zawarcia umowy lub/i jej realizacji, zlecenia usług lub zamówienia dostaw oraz ich realizacji. Ich niepodanie może uniemożliwić realizację ww. czynności.

- **INFORMACJA W ZAKRESIE ZAUTOMATYZOWANEGO PODEJMOWANIA DECYZJI ORAZ PROFILOWANIA**

Państwa dane nie posłużą do zautomatyzowanego podejmowania decyzji jak również profilowania.

Załącznik nr 2 do umowy o zachowaniu poufności (3b)

……
(imię i nazwisko)

……
(nazwa Wykonawcy, adres siedziby)

OŚWIADCZENIE
o zobowiązaniu do zachowania poufności
dla pracownika Wykonawcy

Ja niżej podpisany, reprezentujący Wykonawcę podczas realizacji umowy **nr ……/2019** w siedzibie Łódzkiego Oddziału Wojewódzkiego NFZ, z uwagi na udostępnianie Informacji Poufnych, zobowiązuje się do:

1) zachowania w tajemnicy wszystkich Informacji Poufnych uzyskanych podczas realizacji umowy, przedmiotem której jest **zakup systemu do ochrony przed wyciekiem danych (DLP)**, w okresie realizacji zamówienia, a także po wygaśnięciu lub rozwiązaniu umowy, niezależnie od formy w jakiej zostały mi przekazane;
2) wykorzystywania Informacji Poufnych uzyskanych podczas realizacji umowy wyłącznie w celu realizacji umowy.

…… ……
miejscowość, data czytelny podpis

KLAUZULA INFORMACYJNA
DOTYCZĄCA PRZETWARZANIA W ŁÓDZKIM ODDZIALE WOJEWÓDZKIM NFZ DANYCH OSOBOWYCH PRACOWNIKÓW KONTRAHENTA W ZWIĄZKU Z ZAWARCIEM I REALIZACJĄUMOWY (Pzp) (3b)

Zgodnie z art. 14 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne rozporządzenie o ochronie danych, dalej: RODO) - Łódzki Oddział Wojewódzki NFZ informuje:

- **ADMINISTRATOR DANYCH OSOBOWYCH**

Narodowy Fundusz Zdrowia, reprezentowany przez Dyrektora Łódzkiego Oddziału Wojewódzkiego NFZ, w zakresie danych osobowych przetwarzanych w Oddziale Wojewódzkim, z którym mogą się Państwo skontaktować w następujący sposób:

- listownie na adres siedziby administratora: ul. Kopcińskiego 58, 90-032 Łódź,
- za pomocą platformy ePUAP
- e-mailem: sekretariat@nfz-lodz.pl.

- **INSPEKTOR OCHRONY DANYCH**

W sprawach dotyczących przetwarzania Państwa danych przez Łódzki Oddział Wojewódzki NFZ można kontaktować się z Inspektorem Ochrony Danych w następujący sposób:

- listownie na adres siedziby administratora: ul. Kopcińskiego 58, 90-032 Łódź**,**
- telefonicznie: (42) 275 40 28,
- e-mailem: IOD@nfz-lodz.pl.

- **CEL I PODSTAWY PRZETWARZANIA**

Państwa dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. f RODO w celu zapewnienia prawnie uzasadnionego interesu administratora polegającego na możliwości realizacji umowy zawartej w wyniku postępowania o udzielenie zamówienia publicznego na **zakup systemu do ochrony przed wyciekiem danych (DLP)** w siedzibie Łódzkiego Oddziału Wojewódzkiego Narodowego Funduszu Zdrowia (nr postępowania: ZP/ŁOW NFZ/6/2019), prowadzonego zgodnie z ustawą z dnia 29 stycznia 2004 r. prawo zamówień publicznych (dalej:„Pzp") oraz zapewnieniu ochrony informacji udostępnionych w związku z wykonywaniem umowy.

- **ODBIORCY DANYCH OSOBOWYCH**

Odbiorcami Państwa danych osobowych mogą być podmioty posiadające upoważnienie do pozyskiwania tych danych na podstawie przepisów prawa powszechnie obowiązującego. Dane osobowe mogą zostać przekazane podmiotom, z którymi administrator danych osobowych zawarł umowę powierzenia przetwarzania danych osobowych. Administrator danych osobowych nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego

- **ŹRÓDŁO I KATEGORIE DANYCH OSOBOWYCH**

Administrator pozyskał Państwa dane osobowe w zakresie ……..(wpisać kategorie danych) od ……..……..… z siedzibą w ……..……..… przy ul. ……..……..……,

- **OKRES PRZECHOWYWANIA DANYCH**

Państwa dane osobowe będą przechowywane do chwili realizacji zadania, do którego zostały zebrane oraz przez czas niezbędny do obrony roszczeń, a także przez czas wynikający z przepisów ustawy o narodowym zasobie archiwalnym i archiwach.

- **PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ**

W odniesieniu do danych przetwarzanych we wskazanym celu osobie, której dane dotyczą przysługuje:

- prawo dostępu do treści swoich danych;
- prawo do sprostowania danych;
- prawo do ograniczenia przetwarzania;
- prawo do wniesienia sprzeciwu wobec przetwarzania;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Każde z w/w żądań zostanie indywidualnie rozpatrzone, zgodnie z RODO.

- **INFORMACJA O WYMOGU PODANIA DANYCH**

Podanie przez Państwa danych osobowych jest niezbędne dla realizacji postanowień umowy, zawartej
w wyniku postępowania o udzielenie zamówienia publicznego.

- **INFORMACJA W ZAKRESIE ZAUTOMATYZOWANEGO PODEJMOWANIA DECYZJI ORAZ PROFILOWANIA**

Państwa dane nie posłużą do zautomatyzowanego podejmowania decyzji jak również profilowania.