Znak sprawy: AZP – 2611 – 32/11

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA
DOSTAWA SYSTEMU DO OCHRONY PRZED WYCIEKIEM INFORMACJI W CENTRALI NFZ WRAZ ZE WSPARCIEM TECHNICZNYM

1. NAZWA I ADRES ZAMAWIAJĄCEGO

Narodowy Fundusz Zdrowia Centrala (w skrócie NFZ)
ul. Grójecka 186
02-390 Warszawa

2. TRYB UDZIELENIA ZAMÓWIENIA

Postępowanie jest prowadzone w trybie przetargu nieograniczonego, zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj Dz. U. z 25 czerwca 2010 r. Nr 113, poz. 759 z późn. zm.) zwanej dalej ustawą.

3. OPIS PRZEDMIOTU ZAMÓWIENIA

3.1. Przedmiotem zamówienia jest **dostawa systemu do ochrony przed wyciekiem informacji w Centrali NFZ wraz ze wsparciem technicznym.**
3.2. Zamawiający zastrzega sobie możliwość wezwania wykonawców do przeprowadzenia testów oferowanego systemu weryfikacji świadczeń. Szczegóły dotyczące przeprowadzenia testów opisane są w załączniku Nr 1 do Specyfikacji.
3.3. Szczegółowy opis przedmiotu zamówienia stanowi załącznik Nr 1 do Specyfikacji.
3.4. Szczegółowy zakres praw i obowiązków związanych z realizacją zamówienia określa wzór umowy (załącznik nr 2 do Specyfikacji).
3.5. Zamawiający dopuszcza udział podwykonawców w wykonaniu zamówienia. W przypadku wykonywania części zamówienia przez podwykonawcę Wykonawca wskaże w formularzu ofertowym, stanowiącym załącznik nr 3 do Specyfikacji, część zamówienia, które powierza podwykonawcy.
3.6. Zamawiający nie dopuszcza składania ofert częściowych oraz wariantowych.

4. TERMIN WYKONANIA ZAMÓWIENIA

Zamawiający wymaga, by Wykonawca zrealizował zamówienie w trzech etapach:
1) Etap I - 4 tygodnie od dnia podpisania umowy. Realizacja Etapu I odbywać się będzie zgodnie z wymaganiami określonymi w **Załączniku nr 1** do Specyfikacji.
2) Etap II, - do dnia 30 czerwca 2012 roku. Realizacja Etapu II odbywać się będzie zgodnie z wymaganiami określonymi w **Załączniku nr 1** do Specyfikacji.
3) Etap III, obejmujący usługi wsparcia technicznego – 36 miesięcy począwszy od dnia podpisania końcowego protokołu odbioru całego Systemu.

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

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 24 ust. 1 ustawy oraz spełniają warunki udziału w postępowaniu określone w art. 22 ust. 1 ustawy dotyczące:
1) posiadania uprawnień do wykonania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania,

2) posiadania wiedzy i doświadczenia,

Opis sposobu dokonywania oceny spełniania tego warunku

- wykażą się, że wykonali (a w przypadku świadczeń okresowych lub ciągłych uwzględniane są również wykonywane) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a

jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, co najmniej 2 dostawy polegające na dostawie systemu bezpieczeństwa, **<u>każda o wartości przekraczającej 1.000.000,00 zł brutto</u>** z podaniem ich wartości, przedmiotu, dat wykonania i odbiorców oraz załączenia dokumentów potwierdzających, że dostawy te zostały wykonane lub są wykonywane należycie.

3) dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonywania zamówienia,

Opis sposobu dokonywania oceny spełniania tego warunku

Wykonawca na potrzeby realizacji zamówienia musi dysponować co najmniej 2 osobami spełniającymi poniższe wymagania:

- każda z osób posiada minimum 3 letnie doświadczenie we wdrażaniu rozwiązań klasy DLP,
- każda z osób, powinna wykazać się udziałem w 2 projektach o podobnym zakresie do zamawianego,
- każda z osób posiada certyfikat producenta potwierdzający znajomość oferowanego rozwiązania klasy DLP,
- jedna z osób posiada certyfikat CISSP,
- jedna z osób posiada certyfikat audytora systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001.

4) sytuacji ekonomicznej i finansowej.

Opis sposobu dokonywania oceny spełniania tego warunku

- wykażą się posiadaniem środków finansowych lub zdolności kredytowej w wysokości nie mniejszej niż 1.000.000,00 zł.

Ocena spełniania warunków zostanie dokonana według formuły „spełnia" / „nie spełnia" warunków udziału w postępowaniu w oparciu o informacje zawarte w dokumentach i oświadczeniach zawartych w pkt 6 Specyfikacji. Nie spełnienie warunków udziału w postępowaniu skutkować będzie wykluczeniem Wykonawcy z postępowania.

6. <u>WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW, JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU</u>

6.1. ***<u>W celu potwierdzenia spełniania warunków udziału w postępowaniu Wykonawca zobowiązany jest załączyć do oferty następujące dokumenty i oświadczenia:</u>***

6.1.1. Oświadczenie o spełnianiu warunków udziału w postępowaniu zgodnie z załącznikiem nr 4 do Specyfikacji.

6.1.2. Wykaz wykonanych dostaw wraz z dokumentami, że dostawy te zostały wykonane należycie.

W zakresie wykazania spełniania przez wykonawcę warunków, o których mowa w pkt 5.2) Specyfikacji, oprócz oświadczenia o spełnieniu warunków udziału w postępowaniu, Wykonawca zobowiązany jest przedstawić pisemny wykaz wykonanych usług w zakresie niezbędnym do wykazania spełniania warunku wiedzy i doświadczenia w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, z podaniem ich wartości, przedmiotu, dat wykonania i odbiorców, oraz załączeniem dokumentów potwierdzających, że te usługi zostały wykonane lub są wykonywane należycie.
Wzór wykazu stanowi załącznik nr 6 do Specyfikacji. W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony warunek musi spełniać co najmniej 1 podmiot lub warunek podmioty te mogą spełniać łącznie.

Jeżeli Wykonawca wykazując spełnianie warunku, o którym mowa w pkt 5.2) Specyfikacji polega na wiedzy i doświadczeniu innych podmiotów na zasadach określonych w art. 26 ust. 2b ustawy, zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował zasobami niezbędnymi do

realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonywaniu zamówienia.

6.1.3. Wykaz osób, które będą brały udział w realizacji zamówienia.

Wykonawca zobowiązany jest przedstawić pisemny wykaz osób, które będą uczestniczyć w wykonaniu zamówienia wraz z informacjami na temat ich kwalifikacji niezbędnych do wykonania zamówienia oraz informacją o podstawie do dysponowania tymi osobami (tak jak w załączniku Wykaz osób musi być sporządzony zgodnie z wzorem stanowiącym Załącznik nr 7 do SIWZ. Wykaz musi zawierać informacje niezbędne do stwierdzenia czy Wykonawca spełnia warunek określony w pkt 5.3) SIWZ.

Jeżeli Wykonawca wykazując spełnianie warunku, o którym mowa w pkt 5.3) Specyfikacji polega na wiedzy i doświadczeniu innych podmiotów na zasadach określonych w art. 26 ust. 2b ustawy, zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonywaniu zamówienia.

6.1.4. Dokument potwierdzający wysokość posiadanych środków finansowych lub zdolność kredytową

Dokumentem takim będzie informacja banku lub spółdzielczej kasy oszczędnościowo-kredytowej, w której Wykonawca posiada rachunek, potwierdzającej wysokość posiadanych środków finansowych lub zdolność kredytową Wykonawcy w wysokości nie mniejszej niż 1.000.000,00 zł, wystawionej nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.
Jeżeli Wykonawca wykazując spełnianie warunku, o którym mowa w pkt 5.4 polega na zdolnościach finansowych innych podmiotów na zasadach określonych w art. 26 ust. 2b ustawy, Zamawiający wymaga przedłożenia informacji dotyczącej tych podmiotów.
W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony warunek musi spełniać co najmniej 1 podmiot lub warunek podmioty te mogą spełniać łącznie.

6.2. ***W celu wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia Wykonawca zobowiązany jest załączyć do oferty na podstawie art. 22 ustawy, następujące dokumenty i oświadczenia:***

6.2.1. **Oświadczenie o braku podstaw do wykluczenia** zgodnie z załącznikiem nr 5 do Specyfikacji.

6.2.2. **Aktualny odpis z właściwego rejestru**, jeżeli odrębne przepisy wymagają wpisu do rejestru, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust.1 pkt 2 ustawy, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert, a w stosunku do osób fizycznych oświadczenie Wykonawcy w zakresie art. 24 ust.1 pkt 2 ustawy.

6.2.3. **Dokumenty potwierdzające wywiązywanie się z obowiązków płatności podatków oraz składek na ubezpieczenie zdrowotne i społeczne**

Dokumentami takimi będą aktualne zaświadczenia właściwego naczelnika urzędu skarbowego oraz właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego potwierdzające odpowiednio, że Wykonawca nie zalega z opłacaniem podatków oraz składek na ubezpieczenie zdrowotne i społeczne, lub zaświadczeń, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.

Za aktualne zaświadczenia uznaje się jedynie zaświadczenia wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, dokumenty /zaświadczenia/ muszą być złożone przez każdego Wykonawcę.

6.2.4. Informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 4-8 ustawy

Dokumentem takim będzie aktualna (**wystawiona nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert**) informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 4-8 ustawy.

W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, dokument musi być złożony przez każdego Wykonawcę**.**

6.2.5. Informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 9 ustawy

Dokumentem takim będzie aktualna (**wystawiona nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert**) informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 9 ustawy.

W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, dokument musi być złożony przez każdego Wykonawcę.

6.2.6. Wykonawcy zagraniczni

1) Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczpospolitej Polskiej, zamiast dokumentu, o którym mowa w pkt 6.2. 2, 6.2.3, 6.2.5. - składa dokument lub dokumenty wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania potwierdzające odpowiednio, że:
   a) nie otwarto jego likwidacji ani nie ogłoszono upadłości,
   b) nie zalega z uiszczeniem podatków, opłat, składek na ubezpieczenie społeczne i zdrowotne albo, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,
   c) nie orzeczono wobec niego zakazu ubiegania się o zamówienie,
2) o którym mowa w pkt 6.2.4 – składa zaświadczenie właściwego organu sądowego lub administracyjnego kraju pochodzenia albo zamieszkania osoby, której dokumenty dotyczą, w zakresie określonym w art. 24 ust. 1 pkt 4-8 ustawy.
   Dokumenty, o których mowa w pkt 1 lit a i c oraz w pkt 2 powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert. Dokument, o którym mowa w pkt 1 lit. b powinien być wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.
   Jeżeli w miejscu zamieszkania osoby lub w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt 1 i pkt 2 zastępuje je się dokumentem zawierającym oświadczenie złożone przed notariuszem, właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio miejsca zamieszkania osoby lub kraju , w którym wykonawca ma siedzibę lub miejsce zamieszkania.
3) Jeżeli w przypadku Wykonawcy mającego siedzibę na terytorium Rzeczypospolitej Polskiej, osoby, o których mowa w art. 24 ust. 1 pkt. 5-8 ustawy, mające miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, Wykonawca składa w odniesieniu do nich zaświadczenia właściwego organu sądowego albo administracyjnego miejsca zamieszkania dotyczące niekaralności tych osób w zakresie określonym w art. 24 ust. 1 pkt. 5-8 ustawy, wystawione nie wcześniej niż 6 miesięcy przed upływem terminu podpisania umowy, z tym że w przypadku gdy w miejscu zamieszkania tych osób nie wydaje się takich zaświadczeń- zastępuje się je dokumentem zawierającym oświadczenie złożone przed notariuszem, właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego miejsca zamieszkania tych osób.

6.2.7. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia

a) Wykonawcy ubiegający się wspólnie o udzielenie zamówienia muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Fakt ustanowienia pełnomocnika musi wynikać z załączonych do oferty dokumentów (np. pełnomocnictwa). Dokument pełnomocnictwa musi być złożony w oryginale lub poświadczonej notarialnie za zgodność z oryginałem kopii.
b) Wykonawcy, o których mowa w pkt 1., składają jedną ofertę, przy czym:

a. wymagane oświadczenia lub dokumenty wskazane w pkt 6.2.1 do 6.2.5. składa osobno każdy z Wykonawców,
b. warunek określony w pkt 5.2, 5.3 i 5.4 musi spełniać co najmniej 1 podmiot lub warunek podmioty te mogą spełniać łącznie,
c. załączone do oferty dokumenty muszą być przedłożone w formie oryginałów bądź kserokopii poświadczonej „za zgodność z oryginałem" przez wykonawcę na każdej zapisanej stronie kserowanego dokumentu. Poświadczenie "za zgodność z oryginałem" musi zostać sporządzone przez osoby uprawnione do reprezentowania Wykonawcy - wskazane we właściwym rejestrze lub ewidencji działalności gospodarczej. Podpisy złożone przez Wykonawcę powinny być opatrzone czytelnym imieniem i nazwiskiem lub pieczęcią imienną. Uwaga! każdy z Wykonawców poświadcza "za zgodność z oryginałem" dokumenty, które go dotyczą.

7. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

Zgodnie z art. 38 ustawy, Zamawiający jest obowiązany niezwłocznie udzielić wyjaśnień treści specyfikacji na zasadach określonych w art. 38 ust. 1 i 1b. Treść zapytań wraz z wyjaśnieniami (bez ujawniania źródła zapytania) Zamawiający przekazuje Wykonawcom, którym przekazał Specyfikację, a jeżeli Specyfikacja jest udostępniana na stronie internetowej - zamieszcza na tej stronie.

Zamawiający nie przewiduje zwołania zebrania Wykonawców w celu wyjaśnienia wątpliwości dotyczących treści Specyfikacji.

Zamawiający zastrzega, że zgodnie z art. 38 ust. 4 ustawy w uzasadnionych przypadkach może przed upływem terminu składania ofert zmienić treść specyfikacji. Dokonaną zmianę specyfikacji Zamawiający przekazuje niezwłocznie wszystkim wykonawcom, którym przekazano Specyfikację, a jeżeli Specyfikacja jest udostępniana na stronie internetowej, zamieszcza ją także na tej stronie.

Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują faksem lub drogą elektroniczną.

Uprawnionym do porozumiewania się z wykonawcami pracownikiem Zamawiającego jest Zbigniew Johne Naczelnik Wydziału Inwestycji i Zamówień Publicznych, w dni robocze od poniedziałku do piątku, w godz. 09:00-15:00.

Nr faksu Zamawiającego: 022 572 – 63 – 05, poczta: zamowienia@nfz.gov.pl

Zamawiający przekazywać będzie oświadczenia, wnioski, zawiadomienia oraz informacje faksem lub drogą elektroniczną i żąda niezwłocznego potwierdzania przez Wykonawcę faktu ich otrzymania.

8. WYMAGANIA DOTYCZĄCE WADIUM

1. Wykonawca zobowiązany jest pod rygorem wykluczenia z udziału w postępowaniu wnieść wadium przed upływem terminu składania ofert.
2. Wadium musi być wniesione w wysokości 100.000,00 zł. (słownie: sto tysięcy złotych).
3. Wadium można wnieść w jednej lub kilku formach przewidzianych w art. 45 ust. 6 Ustawy.
4. Jako termin wniesienia wadium uznaje się termin zaksięgowania przelewu na koncie Zamawiającego.
5. Wadium zostanie zwrócone zgodnie z przepisami art. 46 ust 1, 1a i 2 Ustawy.
6. Wadium zostanie zatrzymane wraz z odsetkami, jeżeli zaistnieją okoliczności przewidziane w art. 46 ust. 4a oraz ust. 5 Ustawy.
7. Zamawiający przyjmuje wadium wnoszone w jednej lub kilku następujących formach: w pieniądzu, poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym, gwarancjach bankowych, gwarancjach ubezpieczeniowych, poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t.j. Dz.U. z 2007 Nr 42, poz 275) . Wadium wnoszone w pieniądzu wpłaca się przelewem na rachunek bankowy wskazany przez Zamawiającego.

Dowodem wniesienia wadium będzie:

1) pokwitowanie przelewu kwoty pieniężnej na dobro rachunku Zamawiającego na rachunek bankowy **77 1130 1017 0020 0734 8625 7421,** potwierdzone faktycznym wpływem środków na rachunek przed upływem terminu wnoszenia wadium,
2) dokument potwierdzający zobowiązanie do pokrycia wadium (wadium w formie niepieniężnej).

Wadium wnoszone w innej formie niż w pieniądzu, powinno zawierać bezwzględne i nieodwołalne zobowiązanie podmiotu udzielającego do wypłaty kwoty wadium w przypadkach wymienionych w art. 46 ust. 4a i 5 ustawy.

9. TERMIN ZWIĄZANIA OFERTĄ

Wykonawca jest związany treścią oferty przez okres 60 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
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.
Przedłużenie terminu związania ofertą jest dopuszczalne tylko z jednoczesnym przedłużeniem okresu ważności wadium albo jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą. Jeżeli przedłużenie terminu związania ofertą dokonywane jest po wyborze oferty najkorzystniejszej, obowiązek wniesienia nowego wadium lub jego przedłużenia dotyczy jedynie wykonawcy, którego oferta została wybrana jako najkorzystniejsza.

10. OPIS SPOSOBU PRZYGOTOWANIA OFERT

1. Wykonawca zobowiązany jest załączyć do oferty następujące dokumenty:
   1.1. Krótki opis oferowanego systemu wraz z jego nazwą handlową. Jeżeli oferowana jest część większego systemu, opis powiązań pomiędzy częścią oferowaną i pozostałymi elementami. Jeżeli w skład systemu wchodzi więcej niż jedno rozwiązanie, opis wszystkich rozwiązań i opis integracji pomiędzy nimi.
   1.2. Architekturę logiczną oferowanego systemu z wszystkimi modułami i elementami realizującymi ochronę informacji przed wyciekiem oraz schemat przepływu danych pomiędzy wszystkimi modułami i elementami.
   1.3. Opis poszczególnych ról, jakie realizują moduły i elementy systemu do ochrony przed wyciekiem danych.
   1.4. Schemat i opis architektury fizycznej systemu, w szczególności obejmujący wykaz oprogramowania instalowanego w stacjach roboczych, dedykowanych serwerach oraz parametry tych serwerów.
   1.5. Szczegółowy Opis sposobu integracji z serwerami proxy IronPort oraz systemem poczty elektronicznej Microsoft Exchange Server.
   1.6. Wykaz protokołów sieciowych, które są poddawane analizie pod kątem wykrywania i ochrony przed wyciekiem danych.
   1.7. Wykaz aplikacji (na stacjach roboczych) oraz obsługiwanych formatów plików, które są obsługiwane przez system DLP, tj. poddawane analizie pod kątem wykrywania i ochrony przed wyciekiem danych.
2. Oferta winna być sporządzona zgodnie z treścią formularza oferty załączonego do Specyfikacji. Wykonawca może złożyć ofertę na własnych formularzach, których treść musi być zgodna z formularzami załączonymi do Specyfikacji.
3. **Ofertę** (wypełniony formularz oferty wraz z wymaganymi przez SIWZ oświadczeniami) **muszą podpisać osoby uprawnione** do reprezentowania Wykonawcy - wskazane we właściwym rejestrze lub ewidencji działalności gospodarczej. Ofertę podpisać może pełnomocnik wykonawcy, jeżeli do oferty zostanie załączone pełnomocnictwo do podejmowania określonych czynności, wynikających z ustawy Prawo zamówień publicznych, w postępowaniach o udzielenie zamówień publicznych, w których bierze udział wykonawca, albo szczególne dotyczące niniejszego postępowania. **Dokument pełnomocnictwa musi być złożony w oryginale lub poświadczonej notarialnie za zgodność z oryginałem kopii.** Podpisy złożone przez Wykonawcę powinny być opatrzone czytelnym imieniem i nazwiskiem lub pieczęcią imienną.
4. **Załączone do oferty dokumenty** muszą być przedłożone w formie oryginałów bądź kserokopii poświadczonej „za zgodność z oryginałem" przez wykonawcę na każdej zapisanej stronie kserowanego dokumentu. Poświadczenie "za zgodność z oryginałem" musi zostać sporządzone przez osoby uprawnione do reprezentowania Wykonawcy - wskazane we właściwym rejestrze lub ewidencji

działalności gospodarczej. **Podpisy złożone przez Wykonawcę powinny być opatrzone czytelnym imieniem i nazwiskiem lub pieczęcią imienną**. Uznaje się, że pełnomocnictwo do podpisania oferty obejmuje pełnomocnictwo do poświadczenia za zgodność z oryginałem kopii dokumentów załączanych do oferty. Zamawiający może żądać przedstawienia oryginału lub notarialnie poświadczonej kopii wyłącznie wtedy, gdy złożona przez wykonawcę kopia dokumentu jest nieczytelna lub budzi wątpliwości co do jej prawdziwości.
Uwaga! każdy z Wykonawców poświadcza "za zgodność z oryginałem" dokumenty, które go dotyczą.

5. Każdy wykonawca może złożyć jedną ofertę**.** Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert złożonych przez danego wykonawcę.
6. Ofertę składa się pod rygorem nieważności w formie pisemnej. Zamawiający nie wyraża zgody na złożenie oferty w postaci elektronicznej.
7. Treść oferty musi odpowiadać treści Specyfikacji.
8. Oferta musi być sporządzona w języku polskim, na komputerze lub inną trwałą i czytelną techniką. Poprawki lub zmiany w ofercie muszą być dokonane w sposób czytelny i parafowane przez osobę podpisującą ofertę.
9. Zaleca się, aby oferta wraz z załączonymi do oferty oświadczeniami i dokumentami była zszyta lub spięta (np. zbindowana) i posiadała ponumerowane strony.
10. Dokumenty sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski, poświadczonym przez wykonawcę.
11. Jeżeli oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji powinny one być umieszczone w osobnej wewnętrznej kopercie zatytułowanej **„Dostawa systemu do ochrony przed wyciekiem informacji"**. **Tajemnica przedsiębiorstwa".**
12. Sporządzoną ofertę należy opakować w kopertę oznaczoną dokładną nazwą i adresem wykonawcy oraz napisem **„POSTĘPOWANIE NR AZP -2611 32/11 OFERTA – „Dostawa systemu do ochrony przed wyciekiem informacji" NIE OTWIERAĆ PRZED 28.11.2011 r. GODZ. 10.30".**

11. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

1. Oferty należy składać w zamkniętych kopertach w Narodowym Funduszu Zdrowia Centrala w Warszawie, przy ul. Grójeckiej 186, 02-390 Warszawa, 0.03 **w terminie do dnia 28.11.2011 r.. do godz. 10.00**
2. Złożona oferta zostanie zarejestrowana w ten sposób, że osoba przyjmująca oznaczy kopertę kolejnym numerem oraz odnotuje datę i dokładny czas wpływu. Na żądanie wykonawcy zostanie wydany dowód wpływu oferty, zawierający odcisk pieczęci organizatora postępowania, nazwisko i imię osoby przyjmującej, oznaczenie postępowania oraz datę i dokładny czas wpływu.
3. Jeżeli oferta jest wysyłana za pomocą przesyłki kurierskiej/listowej, Wykonawca winien zaznaczyć, że przesyłka zawiera ofertę oraz wskazać numer postępowania. Zamawiający nie ponosi odpowiedzialności za następstwa spowodowane brakiem zabezpieczenia oferty lub brakiem którejkolwiek z ww. informacji.
4. Zamawiający zastrzega, że wyłączne ryzyko nieterminowego dostarczenia oferty oraz pomyłkowego otwarcia wskutek nienależytego oznaczenia koperty ponosi Wykonawca.
5. Przed upływem terminu składania ofert, Wykonawca może wycofać ofertę lub wprowadzić zmiany do złożonej oferty. Informacja o wycofaniu oferty lub zmiany do oferty Wykonawca winien doręczyć Zamawiającemu na piśmie przed upływem terminu składania ofert. Oświadczenie o wycofaniu oferty lub wprowadzeniu zmian w ofercie winno być opakowane tak jak oferta, a opakowanie winno być dodatkowo oznaczone odpowiednio wyrazem „WYCOFANIE" lub „ZMIANA". Opakowania te będą otwierane w terminie otwarcia ofert, określonym w niniejszej specyfikacji. Koperty oznakowane „WYCOFANIE" będą otwierane w pierwszej kolejności. Po stwierdzeniu poprawności postępowania Wykonawcy, oferty wycofane nie będą otwierane.
6. Otwarcie ofert odbędzie się **w dniu 28.11.2011 r. o godz. 10.30** w Narodowym Funduszu Zdrowia Centrala w Warszawie przy ul. Grójeckiej 186, parter., 0.03

12. OPIS SPOSOBU OBLICZENIA CENY

Zamawiający wymaga, by oferowana cena za realizację przedmiotu zamówienia została wyliczona zgodnie z formułą określoną w formularzu ofertowym. Jako podstawę do oceny ofert Zamawiający przyjmuje cenę brutto (z podatkiem od towarów i usług VAT) za realizację zamówienia.

UWAGA!

Zamawiający wymaga, by oferowana cena została przedstawiona w rozbiciu na etapy, cenę netto, podatek od towarów i usług (VAT) oraz cenę brutto:

- za dostawę sprzętu, licencji, cena dostawy licencji obejmuje koszty instalacji i wdrożenia
- za świadczenie usługi wsparcia techniczne

Jako podstawę do oceny ofert Zamawiający przyjmuje łączną cenę brutto, która w toku postępowania nie może ulec zmianie.

Oferowana cena powinna uwzględniać wszystkie koszty i opłaty Wykonawcy z tytułu wykonania zamówienia. Wszystkie ceny powinny zawierać w sobie ewentualne upusty proponowane przez Wykonawcę (niedopuszczalne są żadne negocjacje cenowe).

Wszelkie rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w PLN.

13. OCENA OFERT

Do oceny ofert zakwalifikowanych jako ważne Zamawiający przyjął kryterium określone w ogłoszeniu o zamówieniu wraz ze wskazaniem jego znaczenia (wagą wyrażoną w % udziale w ocenie oferty).

Zaokrąglenia w obliczeniach końcowych punktacji – do dwóch miejsc po przecinku.

Szczegółowe zasady oceny z tytułu kryterium zostały przedstawione poniżej.

13.1 Kryterium: CENA (100% wagi oceny)

Z tytułu niniejszego kryterium maksymalna liczba punktów wynosi 100.

Oferta o najkorzystniejszej (najniższej) cenie brutto uzyska 100 pkt. Pozostałe ceny obliczone dla badanych ofert zostaną porównane z ofertą o najkorzystniejszej (najniższej) cenie brutto, stosując poniższy wzór:

$$K_m = \frac{C_n}{C_m} \times 100\,pkt$$

Gdzie: $_m$ – oznacza kolejną badaną ofertę,

$\mathbf{K_m}$ – oznacza **wynik oceny kolejnej badanej oferty w zakresie kryterium ceny**,

$\mathbf{C_n}$ – oznacza **najkorzystniejszą (najniższą) cenę brutto badanej oferty,**

$\mathbf{C_m}$ – oznacza **cenę brutto kolejnej badanej oferty.**

13.2 Ocena łączna

Dla każdej oferty wyniki oceny z tytułu kryterium zostaną obliczone według poniższego wzoru.

$$O_l = K_m \times X \times W_C$$

Gdzie: $\mathbf{O_l}$ – oznacza **ocenę łączną oferty**

$\mathbf{K_m}$ – oznacza **wynik oceny kolejnej badanej oferty w zakresie kryterium ceny,**

X – oznacza **niezmienną liczbę członków Komisji przetargowej biorących udział w ocenie,**

$\mathbf{W_c}$ - oznacza **wagę oceny kryterium.**

Zamawiający wybierze ofertę, która uzyska najwyższą liczbę punktów zgodnie z powyższym wzorem.

14. INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

Treść umowy o realizację zamówienia zostanie ustalona zgodnie z treścią wybranej oferty i załączonego do Specyfikacji wzoru umowy.

Zamawiający zawrze umowę w terminie nie krótszym niż 10 dni od dnia przekazania zawiadomienia o wyborze oferty, z zastrzeżeniem art. 94 ust. 2 ustawy.

W zawiadomieniu o wyborze oferty najkorzystniejszej Zamawiający poinformuje Wykonawcę o terminie i miejscu zawarcia umowy. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy muszą posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy.

15. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Wykonawca jest zobowiązany do wniesienia zabezpieczenia należytego wykonania umowy na sumę stanowiącą **2 %** ceny całkowitej /brutto/ podanej w ofercie.
Dopuszczalne są następujące formy zabezpieczenia:
1) w pieniądzu - wpłacane przelewem na konto bankowe Zamawiającego:
77 1130 1017 0020 0734 8625 7421,
2) w poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym, gwarancjach bankowych, gwarancjach ubezpieczeniowych, poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.
Zabezpieczenie może być wnoszone według wyboru Wykonawcy w jednej lub kilku formach.
Kwoty pieniężne wpłacone tytułem zabezpieczenia Zamawiający przechowuje na oprocentowanym rachunku bankowym.
Zamawiający zwraca zabezpieczenie wniesione w pieniądzu z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszonymi o koszty prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.
Wykonawca jest obowiązany wnieść całość zabezpieczenia **najpóźniej w dniu podpisania umowy.** Zwrot zabezpieczenia nastąpi na warunkach określonych w umowie. Wadium wniesione w pieniądzu przez Wykonawcę, którego oferta została wybrana, za zgodą tego Wykonawcy zaliczane jest przez Zamawiającego na poczet zabezpieczenia należytego wykonania umowy. W trakcie realizacji umowy Wykonawca może dokonać zmiany formy zabezpieczenia, na jedną lub kilka form, o których mowa w pkt 1 i 2. Zmiana formy zabezpieczenia jest dokonywana z zachowaniem ciągłości zabezpieczenia i bez zmniejszenia jego wysokości

16. WZÓR UMOWY – ZGODNIE Z ZAŁĄCZNIKIEM NR 2 DO SIWZ

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

Wykonawcom a także innym osobom, których interes prawny, w uzyskaniu zamówienia doznał lub może doznać uszczerbku, w wyniku naruszenia przez zamawiającego przepisów ustawy, przysługują środki ochrony prawnej określone w Dziale VI ustawy.

Do Specyfikacji załączono:

1) opis przedmiotu zamówienia (załącznik nr 1),
2) wzór umowy o wykonanie zamówienia (załącznik nr 2),
3) formularz oferty (załącznik nr 3),
4) szczegółowa specyfikacja cenowo – sprzętowa (załącznik nr 4)
5) formularz oświadczenia o spełnianiu warunków udziału w postępowaniu (załącznik nr 4),
6) formularz oświadczenia o braku podstaw do wykluczenia (załącznik nr 5),
7) formularz wykazu wykonanych dostaw (załącznik nr 6),
8) formularz wykazu osób, które będą brały udział w realizacji zamówienia (załącznik Nr 7)
9) podstawowy zakres informacji przetwarzanych w Centrali NFZ (załącznik Nr 8)
10) scenariusze testów akceptacyjnych (załącznik Nr 9)
11) wzór protokołu odbiór testów (załącznik Nr 10)
12) szczegółowa specyfikacja cenowo – sprzętowa (załącznik nr 11)

ZAŁĄCZNIK NR 1 DO SPECYFIKACJI
(po zawarciu umowy załącznik stanie się załącznikiem nr 1 do umowy).

OPIS PRZEDMIOTU ZAMÓWIENIA

DEFINICJE

- Identyfikacja (angielskie pojęcia równoważne: identification, discovery) – proces identyfikowania informacji, które mogą podlegać ochronie przed wyciekiem informacji. Identyfikacja może odbywać się poprzez wskazanie miejsc (np. zasobu sieciowego, bazy danych), gdzie znajdują się dane organizacji. Często do identyfikacji informacji, które mogą podlegać ochronie wykorzystywane są wyrażenia regularne oraz słowa kluczowe.
- Sygnatura (angielskie pojęcia równoważne: hash, fingerprint) – wartość jednoznacznie identyfikująca chronioną informację. Sygnatura może opisywać chroniony plik, jego fragment czy rekord z bazy danych. Sygnatury chronionych informacji mogą powstać np. w wyniku zarejestrowania dokumentu.
- Wykrywanie (angielskie pojęcie: detection) – proces rozpoznawania informacji, które zdefiniowane są w polityce systemu, jako chronione. Wykrywanie zazwyczaj realizuje moduł sieciowy i agent zainstalowany na stacji roboczej. Informacja chroniona wykrywana jest poprzez porównanie z bazą sygnatur bądź na podstawie innego mechanizmu określającego budowę/strukturę/klasyfikację informacji chronionej.

INFORMACJA O TESTACH W ŚRODOWISKU ZAMAWIAJĄCEGO

1. Zamawiający zastrzega sobie możliwość wezwania wykonawców do zaprezentowania oferowanego rozwiązania, zgodnie ze scenariuszem prezentacji (demonstracji), który zostanie przedstawiony wykonawcom wraz z zaproszeniem do prezentacji. Zamawiający przed wysłaniem zaproszenia w drodze losowania określi kolejność wykonawców prezentujących zaoferowane funkcjonalności. Zamawiający zastrzega, że:
   a) Demonstracja zostanie przeprowadzona w siedzibie Zamawiającego.
   b) Zamawiający zapewni pomieszczenie do przeprowadzenia demonstracji.
   c) Zamawiający, na wniosek Wykonawcy, udostępni w/w pomieszczenie od godziny 7:00, w celu umożliwienia Wykonawcy właściwego podłączenia sprzętu.
   d) W ramach demonstracji przewiduje się dwie przerwy: 15 minutowe
   e) Zamawiający dla każdego z wykonawców przewiduje czas na demonstrację w wymiarze do 5 godzin (nie wliczając ww. przerw), w godzinach od 10:00 do 15:30
   f) Celem demonstracji jest weryfikacja funkcjonalności, przedstawionych w scenariuszu wymaganym przez Zamawiającego.
   g) W przypadku późniejszego rozpoczęcia demonstracji z przyczyn leżących po stronie Wykonawcy, Zamawiający nie przewiduje przesunięcia terminu zakończenia demonstracji.
   h) Z przyczyn leżących po stronie Wykonawcy termin prezentacji nie może ulec przesunięciu.
2. Zamawiający zastrzega sobie prawo sprawdzenia, czy zadeklarowane przez Wykonawcę informacje o posiadanej funkcjonalności oferowanego rozwiązania są zgodne ze stanem faktycznym. Zadeklarowana przez Wykonawcę funkcjonalność zostanie uznana za zgodną ze stanem faktycznym, jeżeli wykonana przez Wykonawcę demonstracja wykaże, że jest ona rzeczywiście zawarta w oferowanym systemie. Zamawiający ma prawo żądać zmiany wartości parametrów, bądź danych wprowadzanych do systemu na wartości podane przez niego, celem sprawdzenia czy opisywana funkcjonalność nie jest symulowana. Demonstracja zostanie wykonana w oparciu o sprzęt informatyczny Wykonawcy.
3. W przypadku braku wykazania przez wykonawcę w trakcie demonstracji, że funkcjonalność zadeklarowana przez wykonawcę w ofercie jest rzeczywiście zawarta w oferowanym systemie, oferta tego Wykonawcy zostanie odrzucona.
4. Wszyscy Wykonawcy zostaną poinformowani odrębnym pismem o kolejności, zgodnie z którą Wykonawcy będą wykonywali demonstracje oraz o scenariuszu demonstracji funkcjonalności, zgodnie z którym będą wykonywali demonstrację.

Zakres testów określony został poniżej w tabeli.

Opis czynności	Potwierdzenie wykonania etapu testu	Uwagi
Utworzenie sygnatur plików podlegających ochronie.		Zamawiający przygotuje i wskaże zasób sieciowy (serwer plików) z plikami, które będą podlegać ochronie.
Przygotowanie i przetestowanie polityki korzystającej z danych utworzonych w poprzednim zadaniu, która wykrywa i blokuje informacje chronione przesyłane w sieci (poczta, www) i kopiowane na zewnętrzne nośniki danych (USB, FireWire, CD/DVD).		Testy powinny wykazać, że system skutecznie wykrywa i blokuje informacje chronione przed wyciekiem. Zamawiający wskaże zakresy danych przesyłanych przez sieć czy kopiowanych na zewnętrzne nośniki.
Przygotowanie i przetestowanie polityki korzystającej z wyrażeń regularnych i słów kluczowych, która wykrywa i blokuje informacje przesyłane w sieci (poczta, www) i kopiowane na zewnętrzne nośniki danych (USB, FireWire, CD/DVD)		Test powinny wykazać, że system skutecznie wykrywa i blokuje informacje chronione przed wyciekiem oraz nie generuje fałszywych alarmów. Zamawiający wskaże słowa kluczowe i wzorce danych (np. PESEL).
Przetestowanie polityki wykrywającej dane chronione znajdujące się na lokalnych dyskach stacji roboczej.		Testy powinny wykazać, że agent nie obciąża procesora oraz pamięci a jego praca nie wpływa negatywnie na działanie stacji roboczej. Testy powinny również wykazać, że agent skutecznie rozpoznaje dane chronione znajdujące się w plikach o formatach excel, doc, xml, inne.
Powiadamianie poprzez wiadomość email w języku polskim użytkownika o incydencie (dotyczy modułu sieciowego) oraz powiadamianie poprzez komunikat w języku polskim na konsoli (dotyczy modułu na stacje robocze).		Testy powinny wykazać, że system umożliwia automatycznie przesyłanie wiadomości email i umożliwia wyświetlanie komunikatów (okno pop-up) na stacji roboczej.
Blokowanie prób przesłania chronionych informacji za pomocą aplikacji zainstalowanych na stacji roboczej.		Testy powinny wykazać, że agent na stacji roboczej skutecznie blokuje próby przesyłania chronionych informacji. Testy powinny również wykazać, że agent nie generuje fałszywych alarmów podczas pracy użytkowników.

Załącznik nr 10 zawiera wzór protokołu odbioru testów.
Warunkiem przystąpienia do testów jest podpisanie przez Wykonawcę umowy o poufności zgodnie z załącznikiem nr 2 do projektu umowy.

I. OGÓLNE WYMAGANIA FUNKCJONALNE

1. System musi składać się z komponentów umożliwiających wykrywanie i ochronę przed wyciekiem informacji przesyłanej przez sieć oraz znajdującej się na stacjach roboczych oraz wysyłanej/kopiowanej ze stacji roboczych.
2. System musi mieć możliwość tworzenia sygnatur dokumentów (rejestracja dokumentu), które będą podlegać ochronie.
3. System musi mieć możliwość tworzenia sygnatur z dokumentów w sposób, który umożliwia wykrycie i zablokowanie wycieku fragmentów chronionej informacji.
4. System musi mieć możliwość tworzenia sygnatur z dokumentu o dowolnym rozmiarze.
5. System musi umożliwiać wykrywanie i blokowanie chronionych danych na podstawie wyrażeń regularnych, ciągów znaków i słów kluczowych.
6. System musi mieć możliwość definiowania wzorca danych podlegających ochronie. System posiada lub umożliwia utworzenie wzorca danych dla PESEL, NIP, REGON, ICD-9 PL.
7. System musi mieć możliwość przesyłania do użytkowników informacji o naruszeniu zasad polityki bezpieczeństwa w języku polskim za pomocą wiadomości email.
8. System musi umożliwiać skanowanie zasobów w poszukiwaniu informacji objętych ochroną.

II. AGENT NA STACJACH ROBOCZYCH

1. Agent musi wykrywać i blokować próby wysyłania chronionej informacji za pomocą przeglądarki internetowej Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera oraz Apple Safari.
2. Agent musi wykrywać i blokować próby wysyłania chronionej informacji z wykorzystaniem protokołów HTTP, HTTPS, FTP oraz Secure FTP.
3. Agent musi wykrywać i blokować próby wysyłania chronionej informacji za pomocą klienta poczty elektronicznej Microsoft Outlook.
4. Agent musi umożliwiać definiowanie skanowań lokalnych zasobów w poszukiwaniu informacji podlegającej ochronie.
5. Agent musi umożliwiać wykrywanie i blokowanie prób skopiowania chronionej informacji na nośniki zewnętrzne takie jak: płyty CD/DVD, dyski zewnętrzne podłączane za pomocą portów USB i FireWire, pamięci Flash/CompactFlash.
6. Agent musi umożliwiać wykrywanie i blokowanie prób kopiowania chronionej informacji na zasoby sieciowe.
7. Agent musi umożliwiać wykrywanie i blokowanie podczas kopiowania chronionej informacji za pomocą dowolnej aplikacji do zarządzania plikami (np. Windows Explorer, Norton/Total/Free Commander) oraz interpretera poleceń cmd.exe.
8. Agent musi wymuszać politykę ochrony informacji również w przypadku, gdy stacja robocza nie jest podłączona do sieci NFZ (tzw. tryb pracy offline).
9. Agent musi wyświetlać użytkownikowi informację w języku polskim o naruszeniu zasad polityki bezpieczeństwa poprzez komunikat na ekranie stacji roboczej (okno pop-up).
10. Agent musi wykrywać informację chronioną na podstawie sygnatur (dokumentów bądź fragmentów dokumentów).
11. Agent musi wykrywać informację chronioną na podstawie wyrażeń regularnych, ciągów znaków i słów kluczowych.
12. Agent musi umożliwiać wykrywanie i blokowanie informacji chronionych znajdujących się w plikach zapisywanych przez aplikacje z pakietu Microsoft Office (w tym w plikach Word XML Document, XPS Document, Word Macro-Enabled Document)
13. Agent musi umożliwiać wykrywanie i blokowanie informacji chronionych znajdujących się w plikach zapisywanych przez aplikacje LibreOffice oraz Open Office.
14. System nie może modyfikować dokumentów, metadanych opisujących właściwości dokumentów ani dodawać lub modyfikować atrybutów systemu plików (z wyłączeniem czasu dostępu do pliku – Last Access Time).

15. System musi umożliwiać blokowanie użycia funkcji „zrzut ekranu” (ang. printscreen).

III.MODUŁ SIECIOWY

1. System musi mieć możliwość działania w trybie pasywnym (monitorowania ruchu) oraz aktywnym (blokowania).
2. System musi wykrywać i blokować informację podlegającą ochronie, która jest przesyłana za pomocą następujących protokołów TCP: HTTP, HTTPS, FTP, SMTP.
3. System musi wykrywać i blokować próby przesłania informacji chronionej z wykorzystaniem serwisów internetowych opartych o Web 2.0 (portale społecznościowe, usługi typu webmail, komunikatory).
4. System musi wykrywać i blokować próby przesłania informacji chronionej w tunelowanym protokole w HTTP.
5. System musi wykrywać i blokować próby przesłania informacji chronionej za pomocą serwisów typu open proxy.
6. System musi wykrywać i blokować próby przesłania chronionej informacji za wykorzystaniem komunikatorów internetowych.
7. System musi wykrywać i blokować próby przesyłania przez sieć dokumentów (np. jako załączników do usług typu webmail).
8. System musi wykrywać i blokować próby przesyłania przez sieć skompresowanych dokumentów, które zawierają chronioną informację, bez konieczności definiowana w polityce typów archiwów, w których dokument może się znajdować.
9. System musi obsługiwać co najmniej następujące formaty kompresujące dane: ZIP (w tym również tworzonych z poziomu systemu operacyjnego Microsoft - Compressed Folders), RAR, 7ZIP, GZIP.
10. System musi wykrywać i blokować próby przesyłania dokumentów Microsoft Office (Word, Excel, PowerPoint), które w nagłówkach i stopkach zawierają słowa kluczowe, na podstawie których odbywa się wykrywanie informacji chronionych.
11. System musi umożliwiać integrację z rozwiązaniami IronPort za pomocą ICAP.
12. System musi, pełniąc funkcje MTA (Mail Transfer Agent), wykrywać i blokować próby przesłania za pomocą protokołu SMTP informacji chronionej.
13. System musi mieć możliwość przedstawiania na konsoli nazwy użytkownika aktualnie zalogowanego na stacji roboczej, której adres IP został wykryty przez moduł sieciowy.
14. System musi wykrywać i blokować informację podlegającą ochronie, która jest przesyłana za pomocą protokołów TCP, która jest zakodowana przy użyciu BASE64.

IV.ADMINISTROWANIE SYSTEMEM

1. System musi umożliwiać dostęp do funkcji w oparciu o role w systemie.
2. System musi pobierać informacje z Active Directory o użytkownikach, grupach, jednostkach organizacyjnych oraz innych atrybutach (dane te mają służyć, jako informacja uzupełniająca dla wykrytych incydentów).
3. System musi umożliwiać budowanie polityk z wykorzystaniem informacji pochodzących z Active Directory (w szczególności informacje o użytkownikach, grupach, jednostkach organizacyjnych)
4. System musi posiadać workflow oraz mechanizmy obsługi incydentów bezpieczeństwa.
5. System musi umożliwiać integrację z rozwiązaniem klasy SIEM – ArcSight. Integracja ma polegać na wysyłaniu logów i zdarzeń w trybie on-line z Systemu DLP do ArcSight’a.
6. System musi przechowywać zdarzenia/incydenty/alerty w bazie danych.
7. System nie może mieć ograniczeń związanych z rozmiarem eksportowanego raportu.

V. USŁUGI WDROŻENIOWE

1. Należy przedstawić harmonogram wdrożenia systemu uwzględniający poszczególne etapy projektu.
2. W ramach projektu wdrożenia systemu Wykonawca dokona instalacji, uruchomienia oraz integracji systemu do ochrony przed wyciekiem informacji z serwerami proxy IronPort, systemem poczty elektronicznej opartej o Microsoft Exchange (wyłączenie w zakresie monitorowania i blokowania poczty wychodzącej do sieci Internet) oraz Active Directory. W etapie II dokona instalacji i uruchomienia systemu do ochrony przed wyciekiem informacji na wszystkich stacjach roboczych w Centrali NFZ.
   Wymagane jest, aby Wykonawca:
   a. dokonał wszelkich niezbędnych zmian w konfiguracji serwerów proxy Ironport, w tym aktualizacji oprogramowania
   b. dokonał instalacji i konfiguracji w dwóch wskazanych przez Zamawiającego lokalizacjach (m. st. Warszawa) modułu sieciowego systemu monitorującego i blokującego wychodzącą pocztę elektroniczną zawierającą chronione informacje.
3. W ramach projektu wdrożenia systemu Wykonawca:
   a. Opracuje politykę dla systemu, która ma chronić przed wyciekiem dane opisane w załączniku 8 do SIWZ.
      Uwaga: Polityka ma zawierać akcję automatycznego powiadamiania użytkownika o wykonaniu działania niezgodnego z polityką bezpieczeństwa NFZ.
   b. Wdroży proces automatycznego skanowania zasobów w celu wykrywania na stacjach roboczych danych podlegających ochronie.
   c. Opracuje procedurę cyklicznego tworzenia/uaktualniania sygnatur chronionych danych z plików znajdujących się na zasobach sieciowych.
   d. Opracuje proces obsługi incydentów bezpieczeństwa związanych z wyciekiem danych. Proces musi zawierać następujące elementy:
      i. Procedurę postępowania w przypadku wykrycia incydentu,
      ii. Procedurę eskalacji w przypadku braku aktywności osób odpowiedzialnych za obsługę incydentów,
      iii. Szablon raportu/raportów zawierających:
         1. Ilość otwartych incydentów w zadanym przedziale czasu
         2. Ilość zamkniętych incydentów w zadanym przedziale czasu
         3. Zestawienie incydentów zawierające informacje o:
            a. użytkowniku/użytkownikach, których dotyczy incydent,
            b. chronionych danych,
            c. statusie incydentu,
            d. sposobie wykrycia incydentu,
            e. osobie/osobach obsługujących incydent.
4. W ramach projektu wdrożenia Wykonawca opracuję następującą dokumentację powykonawczą:
   a. Opis funkcjonowania urządzeń i oprogramowania systemu do ochrony przed wyciekiem danych,
   b. Specyfikację techniczną sprzętu,
   c. Schematy uwzględniające przepływ danych pomiędzy elementami systemu do ochrony przed wyciekiem danych,
   d. Instrukcje instalacyjne i instrukcje obsługi dla administratora systemu do ochrony przed wyciekiem danych,
   e. Instrukcje obsługi dla użytkownika (operatora konsoli do obsługi incydentów),
   f. Inwentaryzację urządzeń i oprogramowania systemu do ochrony, konfigurację systemu do ochrony, opis zaimplementowanych polityk, opis procedur archiwizacji i odtwarzania systemu jak i bazy zdarzeń/incydentów.
5. Wykonawca przeprowadzi szkolenia/warsztaty:
   a. 5-cio dniowe warsztaty techniczne dla administratorów systemu potwierdzone certyfikatem dla 4 osób. Warsztaty zostaną przeprowadzone poza siedzibą NFZ w terminie do dnia 30.06.2012. W trakcie szkolenia Wykonawca zapewni całodzienne wyżywienie, ew. nocleg oraz transport. Warsztaty obejmą: administrację systemem, konfigurację systemu, tworzenie backupów konfiguracji systemu, tworzenia reguł i polityk, tworzenie szczegółowych raportów oraz umiejętność interpretacji raportów, itp.
      Szczegółowy zakres warsztatów będzie ustalony między Wykonawcą i Zamawiającym.

b. Szkolenie dla pracowników Centrali NFZ w siedzibie Zamawiającego w terminie do dnia 30.06.2012, z zakresu obsługi i interpretacji komunikatów sytemu DLP na stacjach końcowych. Liczba szkolonych pracowników nie przekroczy 360 osób. Grupy szkoleniowe nie będą większe niż 100 osób. Szkolenia przeprowadzone zostaną w ciągu 4 dni roboczych w godzinach 10-14. Szczegółowe terminy i zakres szkolenia ustalony zostanie pomiędzy Wykonawcą a Zamawiającym.

6. Kryterium odbioru usługi wdrożenia będzie wykonanie testów akceptacyjnych. Scenariusz testów akceptacyjnych znajduje się w załączniku nr 9.

VI WSPARCIE TECHNICZNE

W ramach usługi wsparcia technicznego wykonawca zapewni:

1. dedykowanego opiekuna do dyspozycji Zamawiającego, który zaznajomi się ze środowiskiem Zamawiającego związanym z działaniem systemu do ochrony przed wyciekiem danych. W przypadku urlopu lub choroby dedykowanego opiekuna dla NFZ, zostanie wyznaczona nowa osoba, która go zastąpi i będzie w stanie równie skutecznie wykonywać swoje obowiązki.
   Do obowiązków dedykowanego opiekuna będzie należeć:
   - podejmowanie działań zapobiegawczych mających na celu minimalizowanie ryzyka wystąpienia problemów z eksploatacją systemu do ochrony przed wyciekiem danych. Wszelkie działania będą uprzednio uzgadniane z Zamawiającego;
   - udzielenie wsparcia Zamawiającemu, przy zgłaszaniu awarii serwisowanych systemu do ochrony przed wyciekiem danych, tak, aby jak najskuteczniej przeprowadzić ewentualne czynności naprawcze;
   - koordynowanie zgłaszanych przez Zamawiającego problemów (związanych bezpośrednio lub pośrednio z systemem do ochrony przed wyciekiem danych), oraz wsparcie i doradztwo w celu ich rozwiązania.
2. W zakresie wsparcia technicznego Zamawiający wymaga usuwania błędów, błędów krytycznych, rozbudowę i przebudowę do nowszych wersji Systemu, wsparcie przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania.
3. wsparcie świadczone na potrzeby Zamawiającego (Centrali NFZ) w trybie 8 godzin dziennie/5 razy w tygodniu (dni robocze).
4. prawo do pobrania nowych wersji i aktualizacji systemu do ochrony przed wyciekiem danych przez 36 miesięcy od podpisania protokołu odbioru,
5. aby czas usunięcia awarii w okresie świadczenia wsparcia technicznego nie przekraczał w przypadku:
   1) błędu krytycznego uniemożliwiającego działania aplikacji – 72 godziny od czasu jego zgłoszenia,
   2) błędu – aplikacja nie posiada pełnej funkcjonalności – 96 godziny od czasu jego zgłoszenia.
6. możliwość zgłoszenie awarii w jednej z niżej wymienionych form:
   - drogą telefoniczną,
   - faxem,
   - pocztą elektroniczną.
5. dodatkowo łączną pulę 40 roboczodni na:
   a. tworzenie i uaktualnianie sygnatur,
   b. tworzenie i modyfikowanie wyrażeń regularnych wykrywających chronione informacje,
   c. tworzenie i modyfikacje dodatkowych polityk ochrony,
   d. weryfikację poprawności procesu automatycznego skanowania zasobów w celu wykrywania danych podlegających ochronie,
   e. testy,
   f. inne dodatkowe prace związane z systemem ochrony przed wyciekiem danych.

VII WYKAZ ELEMENTÓW PODLEGAJĄCYCH OCHRONIE PRZED WYCIEKIEM DANYCH

Lp.	*Element*	*Ilość*
1	Ruch wychodzący z centrali NFZ	40 Mb/s
2	Stacje robocze użytkowników	450
3	Użytkownicy korzystających z poczty elektronicznej	6000
4	Użytkownicy korzystających z serwerów proxy	6000
5	Systemy operacyjne na stacjach roboczych: Microsoft Windows XP, Microsoft Windows 7 (x32/x64)	450
6	Ilość styków z siecią Internet, przez które wysyłana jest poczta elektroniczna (są to dwie fizycznie oddalone od siebie lokalizacje)	2
7	Ilość styków z siecią Internet, przez które przesyłany jest ruch www	1

ZAŁĄCZNIK NR 2 DO SPECYFIKACJI

UMOWA

zawarta w dniu ..... 2011 r. w Warszawie pomiędzy Narodowym Funduszem Zdrowia z siedzibą w Warszawie przy ul. Grójeckiej 186, NIP 107-00-010-57, zwaną dalej ZAMAWIAJĄCYM, reprezentowanym przez:

…….

a

zwaną dalej WYKONAWCĄ, reprezentowaną przez:

…….

W wyniku przeprowadzonego postępowania o udzielenie zamówienia w trybie przetargu nieograniczonego zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. z 25 czerwca 2010 r. Nr 113, poz. 759 z późn. zm.) zawarto umowę następującej treści:

§ 1

1. Przedmiotem niniejszej umowy jest dostawa systemu do ochrony przed wyciekiem informacji w Centrali NFZ zwanego dalej Systemem wraz ze wsparciem technicznym. Szczegółowy opis przedmiotu zamówienia określono w załączniku nr 1.
2. Zamówienie realizowane będzie w następujących etapach:
   1) Etap I, obejmujący dostawę sprzętu oraz licencji niezbędnych do pełnego funkcjonowania Systemu, instalację i wdrożenie części Systemu, która zapewnia ochronę informacji przesyłanych przez sieć w Centrali NFZ.
   2) Etap II, obejmujący instalację i wdrożenie części systemu, która zapewnia ochronę informacji na stacjach roboczych w Centrali NFZ, oraz przeprowadzenie warsztatów zgodnie z zakresem i warunkami opisanymi w Załączniku nr 1:
   3) Etap III, obejmujący świadczenie usługi wsparcia technicznego dla Systemu.
3. Osoby, które będą uczestniczyć w realizacji umowy ze strony Wykonawcy, spełniają wszystkie wymagania Zamawiającego określone w dokumentacji postępowania przetargowego Wykaz osób, które będą uczestniczyć w realizacji umowy, ze strony Wykonawcy, stanowi załącznik nr 7
4. Wykonawca zobowiązuje się do utrzymania pracowników wymienionych w wykazie, o którym mowa w ust. 3, przez cały czas trwania realizacji umowy, a w razie zmiany na danym stanowisku osoba zastępująca będzie posiadała kwalifikacje wymagane przez Zamawiającego, o zmianie Wykonawca niezwłocznie powiadomi Zamawiającego na piśmie.
5. Na żądanie Zamawiającego Wykonawca jest zobowiązany do przedstawienia certyfikatów potwierdzających, że osoby uczestniczące w realizacji zamówienia spełniają wszystkie wymagania Zamawiającego określone w dokumentacji postępowania przetargowego.

§ 2

Zamawiający wymaga, by zamówienie zostało zrealizowane w następujących terminach:

1) Etap I - 4 tygodnie od dnia podpisania umowy. Realizacja Etapu I odbywać się będzie zgodnie z wymaganiami określonymi w **Załączniku nr 1**.
2) Etap II, - do dnia 30 czerwca 2012 roku. Realizacja Etapu II odbywać się będzie zgodnie z wymaganiami określonymi w **Załączniku nr 1**.
3) Etap III, obejmujący usługi wsparcia technicznego – 36 miesięcy począwszy od dnia podpisania końcowego protokołu odbioru całego Systemu.

§ 3

1. Wysokość łącznego wynagrodzenia brutto z tytułu realizacji niniejszej umowy wynosi ……zł (słownie: ……złotych), w tym podatek VAT, w wysokości (słownie: ……. złotych).
2. Wynagrodzenie, o którym mowa w ust. 1 będzie płatne w następujący sposób:
   1) za wykonanie Etapu I i II,:
      a) 70 % sumy cen części A i B szczegółowej specyfikacji cenowo - sprzętowej stanowiącej załącznik nr 6 do umowy …. tj. ……. zł brutto (słownie: ……..), w tym podatek VAT: …… zł (słownie: …….), podstawą wystawienia faktury jest protokół odbioru, zgodnie z

załącznikiem nr 4 podpisany przez osobę upoważnioną ze strony Zamawiającego, potwierdzający wykonanie Etapu I.

b) 30 % sumy cen części A i B szczegółowej specyfikacji cenowo - sprzętowej stanowiącej załącznik nr 6 do umowy tj. ……. zł brutto (słownie: ……..), w tym podatek VAT: …… zł (słownie: …….), podstawą wystawienia faktury jest końcowy protokół odbioru całego Systemu, zgodnie z załącznikiem nr 4 podpisany przez osobę upoważnioną ze strony Zamawiającego, potwierdzający, że System prawidłowo realizuje funkcje wymagane przez Zamawiającego

2) za wykonanie Etapu III, (część C szczegółowej specyfikacji cenowo - sprzętowej stanowiącej załącznik nr 6 do umowy) ……. zł brutto (słownie: ……..), w tym podatek VAT: …… zł (słownie: …….), podstawą wystawienia faktury będzie zaakceptowany przez Zamawiającego, protokół odbioru usługi wsparcia technicznego za właściwy okres umowy sporządzone wg wzoru zawartego w załączniku nr 5 podpisany przez osobę upoważnioną ze strony Zamawiającego.

3. Zapłata kwot, o których mowa w ust. 2 pkt 1 lit. a i b, nastąpi na rachunek bankowy Wykonawcy, wskazany na fakturze w terminie do 21 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury. Za datę zapłaty Strony ustalają dzień, w którym Zamawiający wydał swojemu bankowi polecenie przelewu wynagrodzenia na rachunek bankowy Wykonawcy, wskazany na fakturze.
4. Wynagrodzenie o którym mowa w ust. 2 pkt 2 będzie płatne w ratach przelewem w terminie 21 dni od daty otrzymania prawidłowo wystawionej faktury za trzy kolejne miesiące, wystawionej po ich upływie na konto Wykonawcy wskazane na fakturze. W przypadku rozpoczęcia lub zakończenia usługi w trakcie miesiąca kalendarzowego pierwsza i ostatnia płatność będzie określona stosunkiem liczby dni kalendarzowych od daty rozpoczęcia lub zakończenia usługi, do liczby dni kalendarzowych w danym trzymiesięcznym okresie rozliczeniowym.
5. Ze strony zamawiającego osobą zobowiązaną i upoważnioną do stałego nadzoru nad realizacją niniejszej umowy, a także podpisywania protokołów odbioru, jest Naczelnik Wydziału Eksploatacji Departamentu Informatyki lub osoba przez niego upoważniona.

§4

1. Wykonawca zobowiązuje się do zapewnienia wsparcia technicznego w okresie 36 miesięcy począwszy od dnia podpisania końcowego protokołu odbioru całego Systemu na zasadach określonych w załączniku nr 1.
2. Strony ustalają, że wsparcie techniczne prowadzone będzie w miejscu instalacji Systemu czyli w Centrali NFZ. Wszystkie koszty związane ze świadczeniem wsparcia technicznego ponosi Wykonawca.
3. Zgłoszenie w ramach usługi wsparcia technicznego może nastąpić jedną z niżej wymienionych form:
   - drogą telefoniczną (na numer telefonu …….)
   - faxem (na numer faksu …… …..)
   - pocztą elektroniczną (na adres poczty elektronicznej……)

§ 5

1. Wykonawca oświadcza, że posiada uprawnienia do sprzedaży i udzielania licencji na oferowane oprogramowanie.
2. Wszystkie dokumenty, w szczególności takie jak: raporty, wykresy, rysunki, specyfikacje techniczne, plany, obliczenia oraz dokumenty pomocnicze lub materiały nabyte, zebrane lub przygotowane w ramach realizacji Przedmiotu Umowy będą stanowić wyłączną własność Zamawiającego. Po wykonaniu lub rozwiązaniu Umowy, Wykonawca przekaże wszystkie takie dokumenty Zamawiającemu, w terminie 10 dni. Wykonawca może zatrzymać kopie dokumentów, o których mowa wyżej, pod warunkiem, że nie będzie ich używał do celów nie związanych z Umową, bez uprzedniej pisemnej zgody Zamawiającego.
3. Wykonawca udzieli prawa do korzystania przez Zamawiającego (licencji) w ramach wynagrodzenia określonego w § 3 ust. 2 pkt 1. ze wszystkich utworów i produktów dostarczonych w wyniku realizacji niniejszej Umowy, takich jak: oprogramowanie komputerowe konieczne do wykonania, wdrożenia i eksploatacji przedmiotu Umowy, podręczniki użytkownika, dokumentacja techniczna, z chwilą dokonania odbioru tych utworów i produktów bez zastrzeżeń przez Zamawiającego w ramach Etapów w wyniku, których powstały autorskie majątkowe prawa do utworu, na polach eksploatacji znanych w chwili podpisania Umowy wymienionych w pkt 1-17, oraz prawo własności nośników, na których zostaną wyrażone autorskie prawa majątkowe:
   1) odtwarzanie,
   2) utrwalanie,
   3) wprowadzanie zmian,
   4) trwałe lub czasowe zwielokrotnianie w całości lub części, jakimikolwiek środkami i w jakiejkolwiek formie,
   5) przekazywanie,

6) przechowywanie,
7) wyświetlanie,
8) stosowanie,
9) wprowadzanie do obrotu:
   a) najem,
   b) podnajem,
   c) dzierżawa,
   d) sprzedaż,
10) wprowadzanie do pamięci komputera wraz z prawem dokonywania rozwoju, modyfikacji,
11) tłumaczenie,
12) przystosowanie,
13) zmiany, modyfikacje układu, treści lub jakichkolwiek zmian, z zachowaniem wszystkich pól eksploatacji, określonych w niniejszym paragrafie, na części zmienione/zmodyfikowane,
14) publikacje i wyświetlanie w całości lub w części w Internecie i innych mediach bez ograniczeń,
15) produkcje i rozpowszechnianie przez Zamawiającego wszelkich materiałów promocyjnych w tym reklamowych w nieograniczonym nakładzie,
16) udostępnianie z prawem do korzystania, przekazywania w całości lub części innym osobom fizycznym i prawnym na wszystkich, lub wybranych polach eksploatacji określonych w niniejszym paragrafie,
17) pola eksploatacji określone w art. 50 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631, z późn. zm.):
   a) w zakresie utrwalania i zwielokrotniania utworu – wytwarzanie określoną techniką egzemplarzy utworu, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową,
   b) w zakresie obrotu oryginałem, albo egzemplarzami na których utwór utrwalono – wprowadzenie do obrotu, użyczenie lub najem oryginału albo egzemplarzy,
   c) w zakresie rozpowszechniania utworu w sposób inny niż określony w lit. b) – publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i remitowanie, a także publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym.

§ 6

Wykonawca ponosi odpowiedzialność za działania i zaniechania osób, którym powierzył wykonanie obowiązków wynikających z umowy jak za działanie lub zaniechanie własne.

§ 7

Zamawiający może odstąpić od umowy w terminie 7 dni od dnia stwierdzenia nienależytego jej wykonania lub wykonania jej w sposób sprzeczny z ofertą.

§ 8

1. WYKONAWCA zapłaci Zamawiającemu karę umowną:
   1) za odstąpienie od umowy przez Zamawiającego z powodu okoliczności za które odpowiada Wykonawca w wysokości 10% wynagrodzenia brutto określonego w § 3 ust. 1 umowy,
   2) za opóźnienie w stosunku do terminów określonych w § 2, w wysokości 0,3% łącznego wynagrodzenia brutto określonego w § 3 ust. 1 za każdy dzień opóźnienia,,
   3) za opóźnienie w stosunku do terminów usunięcia awarii, o których mowa w **Załączniku nr 1** ujawnionych w okresie świadczenia wsparcia technicznego w wysokości 0,02% wynagrodzenia brutto określonego w § 3 ust. 1 za każdą godzinę opóźnienia liczoną od czasu wyznaczonego na ich usunięcie.
2. Zamawiającemu przysługuje prawo dochodzenia odszkodowania przewyższającego karę umowną.
3. Zamawiający zastrzega sobie prawo potrącenia naliczonej kary umownej i odszkodowania z przysługującego Wykonawcy wynagrodzenia wynikającego z wystawionej faktury na co Wykonawca wyraża zgodę.

§ 9

Wykonawca wnosi zabezpieczenie należytego wykonania umowy w wysokości 2 % wynagrodzenia brutto, o którym mowa w § 3 ust. 1 umowy tj. .....zł brutto (słownie: .....złotych).
Zwolnienie wniesionego przez Wykonawcę zabezpieczenia nastąpi w ciągu 30 dni od dnia wykonania

zamówienia i uznania przez Zamawiającego za należycie wykonane.

§ 10

1. Wykonawca zobowiąże pisemnie swoich pracowników i pracowników podwykonawców wyznaczonych do realizacji przedmiotu umowy do zachowania tajemnicy odnośnie wszystkich informacji w związku z realizacją przedmiotu niniejszej umowy przez podpisanie zobowiązań według wzoru określonego w załączniku nr 2 i dostarczy takie dokumenty Zamawiającemu wraz z wykazem osób, które będą upoważnione do dostępu do danych i informacji objętych poufnością zgodnie z załącznikiem nr 3, przed przystąpieniem do praktycznej realizacji niniejszej umowy przez danego pracownika Wykonawcy lub pracownika podwykonawcy.
2. W celu wykonania niniejszej umowy Zamawiający udzieli dostępu do danych osobowych gromadzonych przez Zamawiającego, na zasadach określonych w odrębnej umowie o powierzeniu przetwarzania danych osobowych, którą Strony zobowiązują się zawrzeć nie później niż w ciągu 3 dni od podpisania niniejszej umowy. Umowa o powierzeniu przetwarzania danych osobowych zostanie zawarta zgodnie ze wzorem określonym w załączniku nr 3.

§ 11

1. Całkowita odpowiedzialność Wykonawcy z tytułu realizacji niniejszej umowy ograniczona jest do szkód rzeczywiście poniesionych z wyłączeniem utraconych korzyści. Wykonawca nie ponosi odpowiedzialności za szkody powstałe w wyniku działalności Zamawiającego bądź osób trzecich.
2. Żadna ze Stron umowy nie będzie odpowiedzialna za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z umowy spowodowane przez siłę wyższą rozumianą jako zdarzenie zewnętrzne, którego zaistnienia nie można było przewidzieć oraz którego następstwom nie można było zapobiec, mimo dołożenia należytej staranności.
3. W przypadku zaistnienia siły wyższej, Strona, której taka okoliczność uniemożliwia lub utrudnia prawidłowe wywiązanie się z jej zobowiązań niezwłocznie nie później jednak niż w ciągu 3 dni od jej zaistnienia, powiadomi drugą Stronę o takich okolicznościach i ich przyczynie.
4. Jeżeli siła wyższa, będzie trwała nieprzerwanie przez okres 30 dni lub dłużej, Strony mogą w drodze wzajemnego uzgodnienia rozwiązać umowę, bez nakładania na żadną ze Stron dalszych zobowiązań, oprócz płatności należnych z tytułu wykonanych usług.
5. Okres występowania siły wyższej powoduje odpowiednie przesunięcie terminów realizacji określonego rodzaju usług, na realizację których miała ona wpływ.
6. Okoliczności zaistnienia siły wyższej muszą zostać udowodnione przez Stronę, która się na nie powołuje.

§ 12

Wykonawca zobowiązuje się w czasie obowiązywania niniejszej umowy, a także po jej wygaśnięciu lub rozwiązaniu, do traktowania jako poufnych wszelkich informacji, które zostaną mu udostępnione lub przekazane przez Zamawiającego w związku z wykonaniem niniejszej Umowy, nie udostępniania ich w jakikolwiek sposób osobom trzecim bez pisemnej zgody Zamawiającego i wykorzystania ich tylko do celów niezbędnych do realizacji umowy .

§ 13

1. Wykonawca bez uprzedniej pisemnej zgody Zamawiającego nie może dokonywać przeniesienia praw lub obowiązków wynikających z niniejszej umowy na osoby trzecie, ani regulować ich w drodze kompensaty.
2. Wszelkie zmiany i uzupełnienia niniejszej umowy wymagają zachowania formy pisemnej pod rygorem nieważności,
3. Strony wyrażają zgodę na zmianę wynagrodzenia Wykonawcy, o którym mowa w § 3 ust. 1 i 2, w przypadku zmiany stawek podatku od towarów i usług (VAT). Zmiana wynagrodzenia będzie polegać na doliczeniu do ceny netto wynikającej ze złożonej przez Wykonawcę oferty zmienionej stawki podatku VAT od dnia obowiązywania zmiany stawki podatku.
4. Zamawiający wyrazi zgodę na przedłużenie terminu dostawy, o którym mowa w § 2 pkt 1) i 2) jedynie w przypadku zaistnienia okoliczności niezależnych od Wykonawcy. Za okoliczności niezależne od Wykonawcy, Zamawiający uzna w szczególności:
    1) siłę wyższą,
    2) nieprzewidywalne warunki fizyczne dotyczące transportu.
5. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy Kodeksu Cywilnego i ustawy z dnia 29 stycznia 2004 Prawo Zamówień Publicznych oraz inne mające związek z wykonywaniem przedmiotu umowy.

6. Wszelkie spory powstałe w związku z realizacją niniejszej umowy Strony będą starały się rozstrzygnąć polubownie. W przypadku jeżeli rozstrzygnięcie sporu na drodze polubownej okaże się niemożliwe, zostanie on poddany pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby Zamawiającego.
7. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach. W takim wypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania części umowy.
8. Załączniki dołączone do niniejszej umowy stanowią jej integralną część.
9. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa dla Zamawiającego, jeden dla Wykonawcy.

ZAMAWIAJĄCY WYKONAWCA

ZAŁĄCZNIK NR 2 DO UMOWY

UMOWA O ZACHOWANIU POUFNOŚCI

zawarta dnia ……2011 roku w Warszawie pomiędzy:

Narodowym Funduszem Zdrowia z siedzibą w Warszawie przy ul. Grójeckiej 186, NIP 107 – 00 – 010 – 57, reprezentowanym przez:
……. zwanym dalej „Zamawiającym”,
a ……, reprezentowaną przez:
……. zwaną dalej „Wykonawcą”

W związku z podpisaniem umowy nr …… z dnia ……., której przedmiotem jest……., 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:

a) 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,
b) wszelkie rozmowy lub rokowania prowadzone pomiędzy przedstawicielami stron w związku z realizacją umowy oraz przekazywane przez Zamawiającemu w ich trakcie informacje.

§ 2.

1. Z uwagi na udostępnianie Informacji Poufnych Wykonawca, w tym podwykonawcy, zobowiązuje się do:
   a) zachowania w tajemnicy wszystkich Informacji Poufnych, niezależnie od formy ich przekazania;
   b) wykorzystywania Informacji Poufnych wyłącznie na użytek współpracy Stron w zakresie realizacji umowy;
   c) zapewnienia odpowiedniego i bezpiecznego sposobu przechowywania wszystkich uzyskanych Informacji Poufnych w czasie, gdy znajdują się one w posiadaniu Wykonawcy,
   d) na pisemny wniosek Zamawiającego lub w przypadku rozwiązania albo wygaśnięcia umowy, niezwłocznie zwrócić lub zniszczyć na własny koszt wszelkie materiały zawierające jakiekolwiek Informacje Poufne Zamawiającego wraz ze wszystkim kopiami, będącymi w jego posiadaniu.
2. W przypadku naruszeń przez Wykonawcę obowiązków dotyczących Informacji Poufnych, o których mowa w niniejszej Umowie, Wykonawca zapłaci Zamawiającemu karę umowną do wysokości wartości umowy podstawowej za każdą ujawnioną Informację Poufną.
3. Osoby biorące udział w realizacji umowy podstawowej ze strony Wykonawcy złożą oświadczenie zobowiązujące ich do zachowania w tajemnicy Informacji Poufnych według wzoru określonego w załączniku, który Wykonawca przedłoży niezwłocznie Zamawiającemu.

§ 3.

1. Zobowiązania określone w **§** 2 nie mają zastosowania do Informacji Poufnych:
   a) które są w dniu ujawnienia publicznie znane,
   b) których ujawnienie wymagane jest od Strony otrzymującej 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 potwierdza i wyraża zgodę na to, że nie będzie uprawniony do nabycia żadnych praw do Informacji Poufnych przekazanych przez Zamawiającego lub od niego uzyskanych.

§ 5.

Niniejsza Umowa obowiązywać zostaje zawarta na okres zawarcia 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.

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

§ 7.

Zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§ 8.

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

Podpisano w imieniu:

……

Podpisano w imieniu
Narodowy Fundusz Zdrowia

……..

Załącznik do Umowy o zachowaniu poufności

(imię i nazwisko)
(adres zamieszkania)
(nazwa i nr dokumentu tożsamości)

OŚWIADCZENIE

Oświadczam, że zobowiązuję się do zachowania w tajemnicy i poufności Informacji Poufnych udostępnionych mi w ramach realizacji umowy nr …… z dnia ……., której przedmiotem jest …….

Potwierdzam odbiór

_____

Miejscowość, data czytelny podpis

ZAŁĄCZNIK Nr 3 DO UMOWY

UMOWA O POWIERZENIU PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu …… 2011 r. w Warszawie pomiędzy:

Narodowym Funduszem Zdrowia z siedzibą w Warszawie ul. Grójecka 186, reprezentowanym przez Jacka Paszkiewicza – Prezesa Narodowego Funduszu Zdrowia
zwanym dalej **„Zamawiającym”**,

a

……...
zwaną dalej **„Wykonawcą”**.

W związku z podpisaniem umowy nr …… z dnia ……., której przedmiotem jest dostawa systemu do ochrony przed wyciekiem danych, zwanej dalej „umową podstawową”, Strony w celu właściwego zabezpieczenia przetwarzania danych osobowych w celu realizacji umowy podstawowej postanawiają co następuje:

§ 1

1. **Zamawiający** jest administratorem Zbioru Danych Osobowych NFZ, zwanego dalej „Zbiorem”.
2. **Zamawiający** przetwarza dane osobowe w ramach Zbioru wyłącznie w zakresie i w celach przewidzianych przepisami ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2008 Nr 164 poz. 1027 z późn. zm.).
3. **Zamawiający** przetwarza dane osobowe zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.).
4. **Zamawiający** udostępnia **Wykonawcy** dane osobowe wchodzące w skład Zbioru wyłącznie w celu wywiązania się przez **Wykonawcę** z zadań określonych w umowie podstawowej oraz na okres jej realizacji zgodnie z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

§ 2

1. **Wykonawca** przyjmuje w powierzenie przetwarzanie danych osobowych określonych umową podstawową, wchodzących w skład Zbioru, w celu realizacji umowy podstawowej, oraz oświadcza, iż zna i wypełnia obowiązujące w tym zakresie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024) i zobowiązuje się do przetwarzania danych zgodnie z tymi przepisami oraz do zachowania wymaganej staranności w zabezpieczeniu powierzonych mu danych osobowych zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz przepisów wykonawczych.
2. W ramach zabezpieczenia przekazanych danych osobowych do obowiązków **Wykonawcy** należy w szczególności:
   a) stworzenie i stosowanie przy przetwarzaniu danych osobowych odpowiednich procedur i zabezpieczeń technicznych, informatycznych i prawnych wymaganych przepisami prawa,
   b) zapewnienie zawarcia niezbędnych aneksów do umów o pracę z pracownikami zatrudnionymi przy przetwarzaniu danych osobowych,
   c) przeprowadzenie właściwego szkolenia dla osób realizujących umowę podstawową w zakresie wymagającym przetwarzania danych osobowych,
   d) zawarcie z podwykonawcami umów o powierzeniu przetwarzania danych osobowych.

§ 3

Zamawiający wyraża zgodę na przetwarzanie danych osobowych określonych umową podstawową, w zakresie wynikającym z jej realizacji i określonym w § 2 ust. 1, poza siedzibą **Wykonawcy** pod warunkiem stosowania

wymaganych procedur w zakresie bezpieczeństwa i prawidłowości przetwarzania danych osobowych zgodnie z obowiązującym porządkiem prawnym.

§ 4

1. Wykonawca ponosi odpowiedzialność za szkody wyrządzone Zamawiającemu lub osobom trzecim w związku z przetwarzaniem danych osobowych na podstawie niniejszej umowy.
2. W przypadku stwierdzenia przez Zamawiającego bezprawnego przetwarzania danych osobowych ze Zbioru Danych Osobowych NFZ, którego administratorem jest Zamawiający, Wykonawca zapłaci Zamawiającemu karę umowną do wysokości wartości umowy podstawowej za każde ujawnione zdarzenie.
3. Zamawiający zastrzega sobie prawo potrącenia naliczonej kary umownej i odszkodowania z przysługującego Wykonawcy wynagrodzenia wynikającego z wystawionej faktury na co Wykonawca wyraża zgodę.
4. Wykonawca ponosi odpowiedzialność określoną w ust.1 – 2, także po wygaśnięciu niniejszej umowy jak i umowy podstawowej.

§ 5

Wykonawca zobowiązuje się do ochrony powierzonych mu danych osobowych w związku z realizacją umowy podstawowej, do zachowania ich w tajemnicy i nie przekazywania ich osobom trzecim.

§ 6

5. **Wykonawca** wyraża zgodę i zobowiązuje się umożliwić **Zamawiającemu** kontrolowanie **Wykonawcy** i jego podwykonawców oraz pomieszczeń i sprzętu używanego przy przetwarzaniu danych osobowych w zakresie niezbędnym do stwierdzenia prawidłowości stosowanych zabezpieczeń Zbioru zawierających dane osobowe, w związku z realizacją umowy podstawowej.
6. Strony ustalają, że w celu wykonywania uprawnień o których mowa w ust. 1 upoważnieni pracownicy **Zamawiającego** będą mieli w szczególności prawo do:
   a) wstępu, w godzinach roboczych w *Dni Robocze* za okazaniem imiennego upoważnienia, do pomieszczeń, w których przetwarzane są przekazane dane osobowe i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą oraz oceny stosowanych zabezpieczeń zapewniających ich ochronę,
   b) żądania złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego,
   c) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
   d) żądania udostępnienia do kontroli urządzeń służących do przetwarzania danych,
   e) zlecania sporządzania ekspertyz i opinii.
7. W toku kontroli pracownik **Zamawiającego** przeprowadzający kontrolę ma prawo wglądu do zbioru zawierającego dane osobowe jedynie za pośrednictwem upoważnionego przedstawiciela **Wykonawcy** lub jego podwykonawcy.
8. Z czynności kontrolnych pracownik **Zamawiającego** sporządzi protokół, którego jeden egzemplarz doręczy **Wykonawcy** lub jego podwykonawcy.
9. Protokół podpisują upoważniony pracownik **Zamawiającego** i administrator bezpieczeństwa informacji **Wykonawcy** lub podwykonawcy, który może wnieść do protokołu umotywowane zastrzeżenia i uwagi.

§ 7

Po zakończeniu realizacji umowy podstawowej **Wykonawca** oraz działający na jego zlecenie podwykonawcy, zobowiązują się trwale zniszczyć wszystkie udostępniane przez **Zamawiającego** dane osobowe wraz z nośnikami, na których zostały zapisane oraz powiadomić **Zamawiającego** o dokonaniu zniszczenia zbiorów, przekazując mu kopię protokołu zniszczenia.

§ 8

1. W przypadku stwierdzenia, iż niniejsza umowa w części lub w całości jest nieskuteczna prawnie z jakichkolwiek powodów, Strony zobowiązują się do dokonania takich zmian jej treści, by nieskuteczność ową usunąć.
2. Jeżeli w czasie trwania umowy stan prawny, który obowiązywał w czasie zawierania umowy zmieni się w ten sposób, iż znaczenie jakie Strony nadały poszczególnym postanowieniom umowy zmieni się, a z przepisów prawa będzie wynikało, iż nowy stan prawny ma zastosowanie do stosunków prawnych regulowanych umową, Strony zobowiązują się do stosownej zmiany całości lub części umowy, tak aby przywrócić jej pierwotne znaczenie.

§ 9

Strony poddają rozstrzygnięcie sporów powstałych na gruncie niniejszej umowy właściwemu miejscowo ze względu na siedzibę **Zamawiającego** Sądowi powszechnemu w Warszawie.

§ 10

1. W sprawach nieuregulowanych niniejszą umową zastosowanie mieć będą w szczególności odpowiednie przepisy Kodeksu cywilnego, ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
2. Zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§ 11

Niniejszą umowę zawiera się na czas realizacji umowy podstawowej.

§ 12

Umowa została sporządzona w 4 egzemplarzach, po dwa dla każdej ze Stron.

Zamawiający **Wykonawca**

Załącznik nr 1

(imię i nazwisko)

(adres zamieszkania)

(nazwa i nr dokumentu tożsamości)

OŚWIADCZENIE

Oświadczam, że znana jest mi definicja danych osobowych w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101, poz. 926 z późn. zm.) w myśl, której za dane uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Zobowiązuję się:

1) do zachowania w tajemnicy danych przetwarzanych przez Narodowy Fundusz Zdrowia wraz ze sposobami ich zabezpieczenia;
2) nie pozostawiać bez dozoru, ani udostępniać osobom nieupoważnionym dokumentów materialnych (w formie elektronicznej, papierowej itp.) z danymi;
3) nie wykorzystywać ani nie udostępniać nieuprawnionym dokumentacji z danymi do innych celów niż służbowe Narodowego Funduszu Zdrowia;
4) do niezwłocznego zniszczenia, w sposób uniemożliwiający zidentyfikowanie danych, wydrukowanych nadmiarowo, niepotrzebnych lub błędnych dokumentów;
5) w przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych, bezzwłocznie powiadomić Administratora Bezpieczeństwa Informacji Narodowego Funduszu Zdrowia, administratora systemu informatycznego, właściwego ze względu na zaistniały incydent kierownika komórki organizacyjnej w Narodowym Funduszu Zdrowia, a po godzinach urzędowania również ochronę obiektu;
6) przy przetwarzaniu danych, do szczególnej dbałości o zachowanie poufności, integralności i dostępności danych związanych z dokumentami znajdującymi się w obrocie w Narodowym Funduszu Zdrowia, także dotyczących danych pracowników, dokumentacji systemu przetwarzania danych oraz infrastruktury sprzętowo - programowej systemów informatycznych;
7) przy przetwarzaniu danych poza systemem informatycznym, do szczególnej dbałości o zachowanie poufności treści dokumentów, które znajdują się w obrocie w Narodowym Funduszu Zdrowia, oraz przestrzegania zasad dostępu do danych.

Wykonano w 2 jednobrzmiących egzemplarzach

Potwierdzam odbiór 1 egzemplarza

_____

Miejscowość, data czytelny podpis

……, dnia ……

Protokół wykonania Etapu I/Systemu (protokół końcowy)[1]

Dotyczy umowy nr …… zawartej w dniu ……

Strona zlecająca:	**Strona wykonująca:**
……..	…….
……..	…….
……..	…….

Miejsce wykonania:

……..
……..
……..

Zakres prac/sposób wykonania:

……
……
……
……
……

Uwagi strony zlecającej:

……
……
……

Wszelkie prace wykonane zostały poprawnie i zgodnie postanowieniami umowy.
Niniejszy protokół jest podstawą do sporządzenia faktury za wykonane usługi.

Strona zlecająca:	**Strona wykonująca:**
……..	…….

[1] Niepotrzebne skreślić

ZAŁĄCZNIK NR 5 DO
UMOWY

WZÓR PROTOKOŁU ODBIORU WYKONANEJ USŁUGI

WSPARCIA TECHNICZNEGO

PROTOKÓŁ ODBIORU
PEŁNY/CZĄSTKOWY*
Za okres .....

TYTUŁ ZLECENIA I OSOBA ZGŁASZAJĄCA		

Nazwisko i imię

Tytuł zgłoszenia		Data i godzina zgłoszenia problemu	Data i godzina rozpoczęcia realizacji zgłoszenia
Nazwisko i imię			
Data			
Wynik odbioru	Pozytywny* / Negatywny*/		

ZAŁĄCZNIK NR 3 DO SPECYFIKACJI

pieczęć Wykonawcy

....., dnia .....

Oferta
na dostawę systemu do ochrony przed wyciekiem informacji w Centrali NFZ wraz ze wsparciem technicznym

Nazwa Wykonawcy .....

Adres Wykonawcy .....

tel. ..... fax.....

REGON…….. NIP……

1. Oferowana cena za realizację przedmiotu zamówienia:

1) cena netto .....,..... zł
(słownie:.....)
2) podatek od towarów i usług VAT – ..... zł
(słownie: .....)
3) cena brutto .....,..... zł
(słownie:.....)

2. Oświadczenie o akceptacji terminu realizacji zamówienia:

Oświadczam, że bez zastrzeżeń przyjmuję przedstawiony przez Zamawiającego termin realizacji zamówienia, określony w Specyfikacji.

3. Oświadczenie o akceptacji wymagań określających przedmiot zamówienia:

Oświadczam, że akceptuję wszystkie wymagania określone w załączniku nr 1 do Specyfikacji „Opis przedmiotu zamówienia".

4. Oświadczenie o akceptacji warunków płatności:

Oświadczam, że bez zastrzeżeń przyjmuję przedstawione przez Zamawiającego w specyfikacji warunki płatności za realizację zamówienia.

5. Oświadczenie o akceptacji przedstawionych przez Zamawiającego warunków umownych realizacji zamówienia:

Oświadczam, że bez zastrzeżeń przyjmuję przedstawione przez Zamawiającego warunki umowne realizacji zamówienia określone we wzorze umowy załączonym do specyfikacji. Zobowiązuję się w przypadku wyboru naszej oferty do zawarcia umowy na wymienionych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego.

6. Wniesienie przez Wykonawcę na rzecz Zamawiającego wadium przetargowego

Wadium przetargowe zostało wniesione na rzecz Zamawiającego w dniu .....:

☐ w pieniądzu przelewem na rachunek bankowy

☐ w formie ..... .

W razie zaistnienia przesłanek zwrotu wadium, proszę o jego zwrot na:

☐ nr konta ..... .

☐ na adres ..... .

Wykonawca zobowiązany jest załączyć do oferty potwierdzenie wniesienia wymaganego wadium przetargowego (potwierdzenie wpłaty wadium na dobro wskazanego w specyfikacji rachunku Zamawiającego) lub załączyć do oferty dokument **(oryginał)** potwierdzający zobowiązanie do pokrycia wadium (wadium w formie niepieniężnej). Oryginał dokumentu potwierdzający wniesienie wadium w innej formie niż pieniądz należy złożyć wraz z ofertą w oddzielnej wewnętrznej kopercie oznaczonej „WADIUM".

Ponadto:

1. Uważamy się za związanych niniejszą ofertą przez czas wskazany w specyfikacji istotnych warunków zamówienia, czyli przez okres …… dni od daty składania ofert.
2. Oświadczamy, że sposób reprezentowania Spółki lub wykonawców składających ofertę wspólną dla potrzeb niniejszego zamówienia jest następujący:
   ……
   (wypełniają jedynie wykonawcy prowadzący działalność w formie spółki lub składający ofertę wspólną)
3. Oświadczamy, iż – za wyjątkiem informacji i dokumentów zawartych w ofercie na stronach nr _____ - niniejsza oferta oraz wszelkie załączniki do niej są jawne i nie zawierają informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

7. Oświadczenie Wykonawcy o powierzeniu wykonania części zamówienia podwykonawcom

Oświadczamy, że powierzymy wykonanie części zamówienia podwykonawcom zgodnie z poniższym zestawieniem *

Lp.	Części zamówienia, której wykonanie Wykonawca powierzy podwykonawcom

wypełnić tylko w przypadku powierzenia wykonania części zamówienia podwykonawcom

8.Oświadczenie Wykonawcy o przyjęciu zobowiązania do przeprowadzenia testów

Zobowiązuję się do przeprowadzenia testów oferowanego systemu, zgodnie ze scenariuszem określonym w załączniku nr 1 do SIWZ w miejscu i terminie wskazanym przez Zamawiającego

9.Oświadczenie o dokumentach załączonych do oferty:

1……
2…….
3……
4……

.....

Podpis i pieczęć Wykonawcy

ZAŁĄCZNIK NR 4 DO SPECYFIKACJI

....., dnia .....

OŚWIADCZENIE WYKONAWCY O SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU

.....

.....

.....

.....

/nazwa (firma) i adres Wykonawcy/

(w przypadku Wykonawców występujących wspólnie należy wymienić wszystkich Wykonawców)

Stosownie do treści art. 44 w zw. z art. 22 ust. 1 pkt 1-4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2010 r. Nr 113, poz. 759 z późn. zm):

niniejszym oświadczam, że spełniamy warunki udziału w postępowaniu o zamówienie publiczne na:

dostawę systemu do ochrony przed wyciekiem informacji w Centrali NFZ wraz ze wsparciem technicznym

dotyczące:

1) posiadania uprawnień do wykonania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania,
2) posiadania wiedzy i doświadczenia,
3) dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonywania zamówienia,
4) sytuacji ekonomicznej i finansowej.

.....

podpis i pieczęć Wykonawcy*

* - w przypadku Wykonawców występujących wspólnie podpisuje Pełnomocnik lub wszyscy Wykonawcy

pieczęć Wykonawcy

ZAŁĄCZNIK NR 5 DO SPECYFIKACJI

....., dnia .....

OŚWIADCZENIE WYKONAWCY O BRAKU PODSTAW DO WYKLUCZENIA

.....

.....

.....

.....

/nazwa (firma) i adres Wykonawcy/

Oświadczam, że brak jest podstaw do wykluczenia nas z postępowania o udzielenie zamówienia w okolicznościach, o których mowa w art. 24 ust. 1 ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (t.j. Dz. U. z 2010 r. Nr 113, poz. 759 z późn. zm.) w postępowaniu o zamówienie publiczne na:

dostawę systemu do ochrony przed wyciekiem danych w Centrali NFZ wraz ze wsparciem technicznym

.....

podpis i pieczęć Wykonawcy*

* - w przypadku Wykonawców występujących wspólnie oświadczenie składa każdy Wykonawca

ZAŁĄCZNIK NR 6 DO SPECYFIKACJI

pieczęć Wykonawcy

WYKAZ WYKONANYCH DOSTAW

Wykaz wykonanych (a w przypadku świadczeń okresowych lub ciągłych uwzględniane są również wykonywane) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, co najmniej 2 dostaw polegających na dostawie systemu bezpieczeństwa, **każda o wartości przekraczającej 1.000.000,00 zł brutto** z podaniem ich wartości, przedmiotu, dat wykonania i odbiorców oraz załączenia dokumentów potwierdzających, że dostawy te zostały wykonane lub są wykonywane należycie.

Wykaz musi zawierać informacje niezbędne do stwierdzenia, czy Wykonawca spełnia warunek określony w punkcie 5.2 Specyfikacji. Do każdej wykonanej dostawy (wskazanej w wykazie) należy przedstawić dokument potwierdzający, że dostawa ta została wykonana należycie.

Datę wykonania zamówienia należy określić jako miesiąc i rok.

Przedmiot	**Wartość zamówienia /brutto/ w PLN**	**Data wykonania /dzień, miesiąc i rok/**	**Nazwa i adres odbiorcy**
1	**2**	**3**	**4**

Uwaga ! Wszystkie wartości należy podać w PLN.

Wykonawcy zobowiązani są załączyć do oferty dokumenty potwierdzające, że wskazane w wykazie dostawy zostały wykonane należycie.

.....

Podpis i pieczęć Wykonawcy

ZAŁACZNIK NR 7 SPECYFIKACJI
(po podpisaniu umowy
stanie się załącznikiem nr 7 do umowy

/nazwa (firma) i adres Wykonawcy/

WYKAZ OSÓB, KTÓRE BĘDĄ UCZESTNICZYĆ W WYKONYWANIU ZAMÓWIENIA

Wykonawca winien przedstawić pisemny wykaz osób, które będą wykonywać zamówienie wraz z informacjami na temat ich kwalifikacji.

lp.	Imię i nazwisko	Kwalifikacje niezbędne do wykonania zamówienia Posiadane certyfikaty Doświadczenie w zakresie określonym w pkt 5.3 (należy podać dane, które potwierdzą spełnienie warunków wymaganych tj. co najmniej nazwa projektu, nazwa firmy dla której realizowany był projekt, okres realizacji,)	Podstawa do dysponowania daną osobą[2)]
1			
2			
3			
4			
5			
6			
7			
8			

Oświadczam, że zobowiązuję się do utrzymania pracowników wymienionych w ww. wykazie przez cały czas trwania realizacji umowy, a w razie zmiany na danym stanowisku osoba zastępująca będzie posiadała kwalifikacje, o których mowa w specyfikacji, o czym powiadomię niezwłocznie Zamawiającego na piśmie.

.....
Podpis i pieczęć Wykonawcy

UWAGA:

1.) osoby przedstawione do realizacji zamówienia muszą spełniać minimalne warunki określone w pkt. 5.3 Specyfikacji
2.) wpisać podstawę do dysponowania daną osobą. Wykonawca zobowiązany jest przedstawić pisemne zobowiązanie innych podmiotów do udostępnienia osób zdolnych do wykonania zamówienia, jeżeli wskazał, że będzie nimi dysponował.

Podstawowy zakres informacji przetwarzanych w Centrali NFZ

Poniżej przedstawiono podstawowy zakres informacji chronionych, które są przetwarzane w Centrali NFZ. Na etapie wdrażania systemu DLP Zamawiający wskaże precyzyjny zakres informacji chronionych uznawanych za wrażliwe, które będą podlegać ochronie przed wyciekiem przez wdrożony system DLP. Wykonawca współdziałając z Zamawiającym określi dokładną charakterystykę przetwarzanych informacji, która będzie odzwierciedlona w politykach systemu DLP.

Zakres przetwarzanych danych związanych ze świadczeniami opieki zdrowotnej:

- Zgodnie z zapisami Art. 188. Pkt 4 Ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, NFZ ma prawo do przetwarzania następujących danych osób uprawnionych do świadczeń opieki zdrowotnej:
    1. nazwisko i imię (imiona);
    2. nazwisko rodowe;
    3. data urodzenia;
    4. płeć;
    5. obywatelstwo;
    6. numer PESEL;
    7. numer NIP - w przypadku osób, którym nadano ten numer;
    8. seria i numer dowodu osobistego, paszportu lub innego dokumentu stwierdzającego tożsamość - w przypadku osób, które nie mają nadanego numeru PESEL lub numeru NIP;
    9. adres zamieszkania;
    10. adres czasowego miejsca pobytu na terytorium Rzeczypospolitej Polskiej, jeżeli dana osoba nie ma na terytorium Rzeczypospolitej Polskiej miejsca zamieszkania;
    11. numer ubezpieczenia;
    12. stopień pokrewieństwa z opłacającym składkę;
    13. stopień niepełnosprawności - w przypadku członka rodziny;
    14. rodzaj uprawnień oraz numer i termin ważności dokumentu potwierdzającego uprawnienia osób do świadczeń opieki zdrowotnej, a także osób posiadających na podstawie odrębnych przepisów szersze uprawnienia do świadczeń opieki zdrowotnej niż wynikające z ustawy;
    15. dane dotyczące udzielonych świadczeń opieki zdrowotnej świadczeniobiorcom;
    16. dane dotyczące przyczyn udzielonych świadczeń opieki zdrowotnej;
    17. nazwa instytucji właściwej osoby uprawnionej do świadczeń opieki zdrowotnej na podstawie przepisów o koordynacji;
    18. dane dotyczące lekarza lub felczera wystawiającego receptę na refundowane leki lub wyroby medyczne;
    19. dane dotyczące świadczeniodawcy zatrudniającego lekarza lub felczera;
    20. dane dotyczące apteki realizującej receptę na refundowane leki i wyroby medyczne;
    21. data zgłoszenia do ubezpieczenia zdrowotnego;
    22. data wyrejestrowania z ubezpieczenia zdrowotnego;
    23. okres, za który opłacono składkę na ubezpieczenie zdrowotne;
    24. dane o płatniku składki na ubezpieczenie zdrowotne;
    25. typ dokumentu uprawniającego do świadczeń opieki zdrowotnej;
    26. data zgonu.

- Zgodnie z zapisami Art. 188a. Ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, NFZ ma prawo do przetwarzania następujących danych osób udzielających świadczeń na podstawie umów o udzielenie świadczeń opieki zdrowotnej oraz ubiegających się o zawarcie takich umów:
    1. nazwisko i imię (imiona);
    2. nazwisko rodowe;
    3. numer PESEL, a w przypadku jego braku - numer dokumentu potwierdzającego tożsamość;
    4. numer prawa wykonywania zawodu - w przypadku osób, którym nadano ten numer;
    5. dotyczących kompetencji zawodowych istotnych z punktu widzenia udzielania świadczeń opieki zdrowotnej na podstawie umowy z Funduszem.

- Zgodnie z zapisami Art. 191. Pkt 3 Ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, NFZ ma prawo do przetwarzania następujących danych świadczeniobiorców innych niż ubezpieczeni:
    1. nazwisko i imię;
    2. numer PESEL;
    3. numer NIP - w przypadku osób, którym nadano ten numer;
    4. seria i numer dowodu osobistego lub paszportu - w przypadku osób, które nie mają nadanego numeru PESEL lub numeru NIP;
    5. dane dotyczące rodzaju i zakresu udzielonych świadczeniobiorcom innym niż ubezpieczeni świadczeń opieki zdrowotnej.

Zakres przetwarzanych danych powiązanych ze świadczeniami opieki zdrowotnej:

- Statystyki (agregaty) z danych związanych ze świadczeniami opieki zdrowotnej,
- Analizy (raporty) z danych związanych ze świadczeniami opieki zdrowotnej,
- Międzynarodowa klasyfikacja procedur medycznych (ICD-9),
- Słowniki: m.in. dotyczące zakresów świadczeń, rodzajów świadczeń,
- Listy oczekujących na świadczenia.

Zakres przetwarzanych danych finansowo-księgowych:

- Koszty z wykonanych świadczeń,
- Plany finansowe NFZ.

Zakres przetwarzanych danych kadrowo-płacowych:

- Zbiór danych osobowych pracowników NFZ oraz osób współpracujących z NFZ na zasadach innych niż umowa o pracę (np. praktykanci),
- Zbiór danych płacowych pracowników NFZ oraz osób współpracujących z NFZ na zasadach innych niż umowa o pracę.

Zakres przetwarzanych danych kontraktowych:

- Umowy zawarte z podmiotami realizującymi zlecenia na rzecz NFZ.

Zakres przetwarzanych danych stanowiących tajemnicę przedsiębiorstwa:

- Hasła dostępowe,
- Klucze kryptograficzne,
- Schematy sieci,
- Dokumentacja techniczna systemów informatycznych,
- Dokumentacja bezpieczeństwa.

Zakres i cel testów akceptacyjnych

Testy akceptacyjne systemu DLP przeprowadzane są w celu weryfikacji czy wdrożone rozwiązanie prawidłowo realizuje funkcje wymagane przez Zamawiającego w zakresie wykrywania wycieków informacji.
Testy akceptacyjne będą przeprowadzane przez Wykonawcę pod nadzorem przedstawicieli Zamawiającego, będącymi członkami Zespołu powołanego w celu dokonania odbioru wdrożonego systemu DLP.

Kryteria rozpoczęcia, zawieszenia, wznowienia i zakończenia testów

Warunkiem do rozpoczęcia procedury testów akceptacyjnych w uzgodnionym pomiędzy stroną Zamawiającego i Wykonawcy terminie, jest pozytywne przejście odbioru ilościowego dostarczonego sprzętu, który nie jest przedmiotem niniejszego modelu testów akceptacyjnych.
Testy akceptacyjne będzie uważało się za zakończone, jeżeli zostaną wykonane wszystkie zaplanowane scenariusze testowe, obejmujące poszczególne przypadki testowe.
Jeżeli zespół realizujący testy stwierdzi wystąpienie przeszkód (na przykład błędne działanie sprzętu lub oprogramowania) uniemożliwiających zakończenie realizacji testów, testy zostaną zawieszone.
W przypadku zawieszenia testów, w uzgodnionych pomiędzy stroną Zamawiającego i Wykonawcy terminie, zostaną usunięte przeszkody uniemożliwiające dokończenie testów i testy zostaną wznowione w zakresie wskazanym przez Zamawiającego.

Wyniki realizacji testów i kryteria akceptacji

Zespół powołany w celu dokonania odbioru wdrożonego systemu DLP dokonuje oceny poprawności realizacji poszczególnych scenariuszy testów. Ocena przyznawana jest w trzy stopniowej skali:

- Akceptacja – dany scenariusz testowy w całości został zakończony pozytywnie zgodnie z kryteriami poprawności zdefiniowanymi w poszczególnych przypadkach testowych wchodzących w skład scenariusza.
- Akceptacja warunkowa – w trakcie realizacji danego scenariusza testu zostały wykryte błędy, które nie blokują dalszej realizacji testów, ale uzyskiwane rezultaty odbiegają od zdefiniowanych kryteriów poprawności w poszczególnych przypadkach testowych. W tym przypadku, Wykonawca zobowiązany jest do dokonania stosowanych korekt lub zaimplementowania alternatywnych rozwiązań, które pozwolą osiągnąć zdefiniowane kryteria poprawności.
- Brak akceptacji – w trakcie realizacji danego scenariusza testów zostały wykryte błędy, które uniemożliwiają dalszą realizację scenariusza i dany scenariusz testowy jest przerywany.

Wymagane zasoby

<do określenia na etapie ustalania szczegółów realizacji testów>

Środowisko testowe

<do określenia na etapie ustalania szczegółów realizacji testów>

Lista scenariuszy testowych

W poniższych tabelach zawarto listy scenariuszy testowych odnoszących się do systemu DLP. Przypadki testowe uwzględniane w poszczególnych scenariuszach przedstawione są w Załącznikach A, B i C.
<W zależności od wdrożonej polityki bezpieczeństwa w systemie DLP przypadki testowe (w zakresie zdefiniowania oczekiwanych wyników i kryteriów poprawności) mogą wymagać dostosowania>

Lista scenariuszy testowych modułu sieciowego

Identyfikator scenariusza testowego	Opis scenariusza testowego	Lista przypadków testowych wchodzących w skład scenariusza testowego
ST_DLP_T-01	Wykrycie i zablokowanie informacji wrażliwych przesyłanych z wykorzystaniem zewnętrznej poczty elektronicznej dostępnej przez przeglądarkę WWW.	PT_DLP_T-01 PT_DLP_T-02 PT_DLP_T-03
ST_DLP_T-02	Wykrycie i zablokowanie informacji wrażliwych przesyłanych na zewnątrz organizacji z wykorzystaniem wewnętrznego systemu poczty elektronicznej.	PT_DLP_T-04 PT_DLP_T-05
ST_DLP_T-03	Wykrycie i zablokowanie informacji wrażliwych przesyłanych na zewnątrz organizacji komunikatorem internetowym.	PT_DLP_T-06 PT_DLP_T-07

ST_DLP_T-04	Wykrycie i zablokowanie informacji wrażliwych umieszczanych w zewnętrznym serwisie internetowym.	PT_DLP_T-08
ST_DLP_T-05	Wykrycie i zablokowanie informacji wrażliwych w jednym z oficjalnych języków w Unii Europejskiej, innym niż polski, przesyłanych na zewnątrz organizacji.	PT_DLP_T-09
ST_DLP_T-06	Wykrycie i zablokowanie informacji wrażliwych przesyłanych ukrytym kanałem na zewnątrz organizacji.	PT_DLP_T-10
ST_DLP_T-07	Wykrycie i zablokowanie informacji wrażliwych poprzez rejestrację dokumentów w systemie DLP.	PT_DLP_T_11 PT_DLP_T_12
ST_DLP_T-08	Wykrycie i zablokowanie informacji wrażliwych na podstawie oznaczeń klasyfikacji informacji.	PT_DLP_T_13
ST_DLP_T-09	Powiadomienie w języku polskim użytkownika o incydencie.	PT_DLP_T_14

Lista scenariuszy testowych modułu agenta

Identyfikator scenariusza testowego	Opis scenariusza testowego	Lista przypadków testowych wchodzących w skład scenariusza testowego
ST_DLP_U-01	Wykrycie i zablokowanie informacji wrażliwych kopiowanych na zewnętrzny nieautoryzowany nośnik.	PT_DLP_A-01
ST_DLP_U-02	Wykrycie i zablokowanie informacji wrażliwych przesyłanych połączniem GRPS/UMTS.	PT_DLP_A-02
ST_DLP_U-03	Wykrycie i zablokowanie informacji wrażliwych przesyłanych połączniem sieci bezprzewodowej WiFi.	PT_DLP_A-03
ST_DLP_U-04	Wykrycie i zablokowanie informacji wrażliwych przenoszonych pomiędzy aplikacjami.	PT_DLP_A-04
ST_DLP_U-05	Wykrycie informacji wrażliwych zapisywanych na lokalnym dysku stacji roboczej.	PT_DLP_A-05
ST_DLP_U-06	Wykrycie i zablokowanie informacji wrażliwych drukowanych na drukarce.	PT_DLP_A-06
ST_DLP_U-07	Możliwość wprowadzania wyjaśnień przez użytkownika.	PT_DLP_A-01–07 (1) PT_DLP_A-07
ST_DLP_U-08	Wykrycie i zablokowanie informacji wrażliwych kopiowanych na sieciowy zasób dyskowy	PT_DLP_A-08

Lista scenariuszy testowych modułu zarządzania

Identyfikator scenariusza testowego	Opis scenariusza testowego	Lista przypadków testowych wchodzących w skład scenariusza testowego
ST_DLP_M-01	Integracja systemu DLP z Active Directory.	PT_DLP_T-01 PT_DLP_M-01
ST_DLP_M-02	Integracja systemu DLP z systemem SIEM.	PT_DLP_T-01 PT_DLP_M-02

Załącznik A. Definicja przypadków testowych dla modułu sieciowego

Identyfikator przypadku testowego	PT_DLP_T-01
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych zawartych w testowym pliku .xls przesyłanym w postaci skompresowanej do archiwum .zip. Plik archiwum jest wysyłany poprzez zewnętrzną pocztę elektroniczną dostępną poprzez przeglądarkę WWW (np. onet lub gazeta). Dostęp do poczty realizowany jest z wykorzystaniem protokołu HTTP.
Zbiór wartości wejściowych	Plik .xls z informacjami wrażliwymi skompresowany do archiwum .zip. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Użytkownik zalogowany do serwisu poczty internetowej. Komunikacja z serwisem pocztowym realizowana protokołem HTTP. Plik z informacjami wrażliwymi przesyłany w postaci załącznika.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za zarządzanie incydentami.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-02
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych zawartych w testowym pliku .xlsx. Plik testowy jest wysyłany poprzez zewnętrzną pocztę elektroniczną dostępną poprzez przeglądarkę WWW (np. gmail). Dostęp do poczty realizowany jest z wykorzystaniem protokołu HTTPS.
Zbiór wartości wejściowych	Plik .xlsx z informacjami wrażliwymi. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Użytkownik zalogowany do serwisu poczty internetowej. Komunikacja z serwisem pocztowym realizowana protokołem HTTPS. Plik z informacjami wrażliwymi przesyłany w postaci

	załącznika.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji i zablokować możliwość wysłania wrażliwych informacji pomimo zastosowania kryptograficznej ochrony informacji (protokół HTTPS). System powinien również wysłać powiadomienie do właściwych osób odpowiedzialnych za zarządzanie incydentami.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-03
Opis przypadku testowego	Wykrycie i zablokowanie fragmentu informacji wrażliwych przesyłanych w treści wiadomości pocztowej, za pośrednictwem zewnętrznej poczty elektronicznej dostępnej poprzez przeglądarkę WWW (np. onet lub gazeta). Dostęp do poczty realizowany jest z wykorzystaniem protokołu HTTP.
Zbiór wartości wejściowych	Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Użytkownik zalogowany do serwisu poczty internetowej. Komunikacja z serwisem pocztowym realizowana protokołem HTTP. Informacje wrażliwe stanowią treść przesyłanej wiadomości.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-04
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych zawartych w testowym pliku .docx. Plik testowy jest wysyłany na zewnątrz organizacji poprzez wewnętrzny system poczty elektronicznej.
Zbiór wartości wejściowych	Plik .docx z informacjami wrażliwymi. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Test realizowany z wykorzystaniem wewnętrznej poczty elektronicznej.

	Plik z informacjami wrażliwymi przesyłany w postaci załącznika.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-05
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych przesyłanych na zewnątrz organizacji poprzez wewnętrzny system poczty elektronicznej. Informacje wrażliwe przesyłane są w treści wiadomości pocztowej.
Zbiór wartości wejściowych	Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Test realizowany z wykorzystaniem wewnętrznej poczty elektronicznej. Informacje wrażliwe przesyłane w treści wiadomości pocztowej.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-06
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych przesyłanych na zewnątrz organizacji poprzez komunikator internetowy (np. Gadu-Gadu).
Zbiór wartości wejściowych	Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Test realizowany z wykorzystaniem komunikatora internetowego. Informacje wrażliwe stanowią treść przesyłanej wiadomości.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*

Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-07
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych przesyłanych na zewnątrz organizacji poprzez komunikator internetowy (np. Gadu-Gadu). Informacje wrażliwe wysyłane są w postaci pliku .pdf.
Zbiór wartości wejściowych	Plik .pdf zawierający informacje wrażliwe. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Test realizowany z wykorzystaniem komunikatora internetowego. Informacje wrażliwe przesyłane są w postaci pliku .pdf.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-08
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych przy próbie udostępnienia ich w zewnętrznym serwisie internetowym (na przykład blog).
Zbiór wartości wejściowych	Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Test realizowany z wykorzystaniem serwisu internetowego (np. blog). Informacje wrażliwe umieszczane są w treści wiadomości.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość udostępnienia wrażliwych informacji i wysłać

	powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-09
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych zawartych w testowym pliku .doc. Plik jest wysyłany poprzez zewnętrzną pocztę elektroniczną dostępną poprzez przeglądarkę WWW (np. onet lub gazeta). Dostęp do poczty realizowany jest z wykorzystaniem protokołu HTTP. Informacje wrażliwe przygotowane są w jednym z oficjalnych języków Unii Europejskiej.
Zbiór wartości wejściowych	Plik .doc z informacjami wrażliwymi przygotowanymi w jednym z oficjalnych języków Unii Europejskiej (*<do określenia w jakim języku najczęściej jest realizowana wymiana informacji>*). Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Użytkownik zalogowany do serwisu poczty internetowej. Komunikacja z serwisem pocztowym realizowana protokołem HTTP. Plik z informacjami wrażliwymi przesyłany w postaci załącznika.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-10
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych zawartych w testowym pliku .txt przesyłanym w postaci skompresowanej do archiwum .rar. Plik jest wysyłany poprzez zewnętrzną pocztę elektroniczną dostępną poprzez przeglądarkę WWW (np. gmail). Dostęp do poczty realizowany jest z poprzez nawiązanie połączenia do zewnętrznego serwera proxy SSL (poprzez HTTPS) i wywołanie serwisu poczty elektronicznej z wykorzystaniem protokołu HTTPS.
Zbiór wartości wejściowych	Plik .txt z informacjami wrażliwymi skompresowany do archiwum .rar. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia*

	systemu DLP> • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Użytkownik zalogowany do serwisu poczty internetowej. Komunikacja z serwerem proxy SSL realizowana protokołem HTTPS. Komunikacja z serwisem pocztowym realizowana protokołem HTTPS. Plik z informacjami wrażliwymi przesyłany w postaci załącznika.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-11
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych zawartych w dokumencie .doc zarejestrowanym w systemie DLP jako chroniony, wysyłanym na zewnątrz organizacji poprzez wewnętrzny system poczty elektronicznej. Dokument przechowywany jest na sieciowym udziale dyskowym. Rejestracja dokumentu w systemie DLP odbywa się poprzez tworzenie sygnatury dla dokumentu.
Zbiór wartości wejściowych	Plik .doc z informacjami wrażliwymi ulokowany w zasobie sieciowym. Utworzona w systemie DLP sygnatura pliku chronionego. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Dokument wysyłany poprzez wewnętrzny system poczty elektronicznej.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-12

Opis przypadku testowego	Wykrycie i zablokowanie fragmentu informacji wrażliwych pochodzących z zarejestrowanego wcześniej w systemie DLP dokumentu .doc. Informacje wrażliwe wysyłane są na zewnątrz organizacji poprzez wewnętrzny system poczty elektronicznej. Dokument zawierający informacje wrażliwe przechowywany jest na sieciowym udziale dyskowym. Rejestracja dokumentu w systemie DLP odbywa się poprzez tworzenie sygnatury dla dokumentu.
Zbiór wartości wejściowych	Plik .doc z informacjami wrażliwymi ulokowany w zasobie sieciowym. Wybrany fragment informacji wrażliwych. Utworzona w systemie DLP sygnatura pliku chronionego. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Informacje wysyłane poprzez wewnętrzny system poczty elektronicznej.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-13
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych zawartych w pliku (.doc, .xls, .pdf), który we właściwościach lub stopce posiada oznaczenie klasyfikacji informacji, wskazującej wymagany poziom ochrony. Informacje wrażliwe wysyłane są na zewnątrz organizacji poprzez wewnętrzny system poczty elektronicznej.
Zbiór wartości wejściowych	Plik z informacjami wrażliwymi oznakowany daną klasą informacji. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Informacje wysyłane poprzez wewnętrzny system poczty elektronicznej.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania

	wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_T-14
Opis przypadku testowego	Wykrycie i zablokowanie informacji wrażliwych zawartych w dokumencie .docx, wysyłanym na zewnątrz organizacji poprzez wewnętrzny system poczty elektronicznej. O zaistniałym incydencie i podjętych działaniach użytkownik powiadamiany jest w języku polskim drogą poczty elektronicznej.
Zbiór wartości wejściowych	Plik .docx z informacjami wrażliwymi. Szablon komunikatu w języku polskim zdefiniowany w systemie DLP. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP na poziomie sieci. Przygotowane szablony komunikatów powiadomień w j. polskim. Test realizowany ze stacji roboczej pracownika Centrali NFZ. Informacje wysyłane poprzez wewnętrzny system poczty elektronicznej.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do użytkownika, który zainicjował nieuprawnione działanie oraz do właściwych osób po stronie obsługi incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu i podjętych działaniach do użytkownika oraz do właściwych osób po stronie obsługi incydentów.

Załącznik B. Definicja przypadków testowych dla modułu agenta

Identyfikator przypadku testowego	PT_DLP_A-01
Opis przypadku testowego	Wykrycie i zablokowanie próby skopiowania pliku .pdf zawierającego informacje wrażliwe na zewnętrzny nośnik USB. Plik kopiowany jest z dysku lokalnego lub dysku sieciowego.
Zbiór wartości wejściowych	Plik .pdf z informacjami wrażliwymi. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP. Agenci systemu DLP zainstalowani na stacjach roboczych

	użytkowników. Test realizowany na stacji roboczej pracownika Centrali NFZ. Plik z informacjami wrażliwymi zapisywany na nośnik USB.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość skopiowania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_A-02
Opis przypadku testowego	Wykrycie i zablokowanie próby wysłania informacji wrażliwych w postaci pliku .pdf na zewnątrz organizacji poprzez podłączenie do komputera telefonu komórkowego pracującego w trybie modemu.
Zbiór wartości wejściowych	Plik .pdf z informacjami wrażliwymi. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP. Agenci systemu DLP zainstalowani na stacjach roboczych użytkowników. Test realizowany na stacji roboczej pracownika Centrali NFZ. Stacja robocza odpięta jest od sieci wewnętrznej organizacji. Do stacji roboczej podłączony jest telefon komórkowy w trybie modemu. Plik z informacjami wrażliwymi przesyłany jest na zewnątrz organizacji.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_A-03
Opis przypadku testowego	Wykrycie i zablokowanie próby wysłania/udostępnienia informacji wrażliwych w postaci pliku .pdf poprzez sieć bezprzewodową w trybie ad-hoc.
Zbiór wartości wejściowych	Plik .pdf z informacjami wrażliwymi. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu*

	DLP>
Warunki wykonania	Działający system DLP. Agenci systemu DLP zainstalowani na stacjach roboczych użytkowników. Test realizowany na stacji roboczej pracownika Centrali NFZ. Stacja robocza odpięta jest od sieci wewnętrznej organizacji. Stacja robocza ma skonfigurowaną sieć bezprzewodową w trybie ad-hoc. Plik z informacjami wrażliwymi jest kopiowany do innego komputera podłączonego do udostępnionej sieci bezprzewodowej.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość wysłania/udostępnienia wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_A-04
Opis przypadku testowego	Wykrycie i zablokowanie próby skopiowania informacji wrażliwych pomiędzy dwoma aplikacjami z wykorzystaniem mechanizmu schowka systemowego. Aplikacja docelowa, do której będą kopiowane informacje nie jest dozwolona do stosowania w organizacji.
Zbiór wartości wejściowych	Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP. Agenci systemu DLP zainstalowani na stacjach roboczych użytkowników. Test realizowany na stacji roboczej pracownika Centrali NFZ. W teście wykorzystywana jest dozwolona i niedozwolona aplikacja. Informacje wrażliwe kopiowane są przez schowek pomiędzy aplikacjami.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość skopiowania wrażliwych informacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_A-05
Opis przypadku testowego	Wykrycie informacji wrażliwych zapisywanych na lokalnym dysku stacji roboczej użytkownika (np. plik .docx, xlsx, lub .pdf). System DLP podczas skanowania lokalnych zasobów

	identyfikuje informacje wrażliwe i podejmuje działania zdefiniowane w polityce.
Zbiór wartości wejściowych	Plik zawierający informacje wrażliwe (w dowolnym formacie). Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP. Agenci systemu DLP zainstalowani na stacjach roboczych użytkowników. Test realizowany na stacji roboczej pracownika Centrali NFZ. Plik z informacjami wrażliwymi umieszczony jest na lokalnym dysku. Agent systemu DLP skanuje lokalne zasoby dyskowe.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć informacje wrażliwe i wysłać powiadomienie do osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_A-06
Opis przypadku testowego	Wykrycie i zablokowanie próby wydruku informacji wrażliwych na drukarce sieciowej oraz drukarce podłączonej do lokalnego komputera.
Zbiór wartości wejściowych	Plik zawierający informacje wrażliwe (w dowolnym formacie). Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP. Agenci systemu DLP zainstalowani na stacjach roboczych użytkowników. Test realizowany na stacji roboczej pracownika Centrali NFZ. Dostęp do drukarki sieciowej i drukarki lokalnej.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć informacje wrażliwe podczas próby wydruku i wysłać powiadomienie do osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_A-07
Opis przypadku testowego	Wykrycie incydentu związanego z wyciekiem informacji i powiadomienie użytkownika o tym fakcie. Użytkownik wskazuje potrzebę/przyczynę realizacji działań odbiegających od przyjętej polityki bezpieczeństwa.

Zbiór wartości wejściowych	Wartości wejściowe określone w innych przypadkach scenariusza.
Warunki wykonania	Działający system DLP. Agenci systemu DLP zainstalowani na stacjach roboczych użytkowników. Podejmowane są działania z innych przypadków scenariusza.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć informacje wrażliwe i wysłać powiadomienie do użytkownika, który zainicjował działanie odbiegające od przyjętej polityki bezpieczeństwa oraz osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wysłał powiadomienie o zdarzeniu do użytkownika. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Identyfikator przypadku testowego	PT_DLP_A-08
Opis przypadku testowego	Wykrycie i zablokowanie próby przekopiowania pliku .pdf zawierającego informacje wrażliwe na sieciowy zasób dyskowy. Plik zapisywany jest w lokalizacji, w której nie mogą być przechowywane informacje wrażliwe.
Zbiór wartości wejściowych	Plik .pdf z informacjami wrażliwymi. Informacje wrażliwe: • Zakres danych: *<do ustalenia na etapie wdrożenia systemu DLP>* • Struktura: *<do ustalenia na etapie wdrożenia systemu DLP>* • Ilość: *<do ustalenia na etapie wdrożenia systemu DLP>*
Warunki wykonania	Działający system DLP. Agenci systemu DLP zainstalowani na stacjach roboczych użytkowników. Test realizowany na stacji roboczej pracownika Centrali NFZ. Plik z informacjami wrażliwymi zapisywany na sieciowy zasób dyskowy.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji, zablokować możliwość skopiowania wrażliwych informacji do niedozwolonej lokalizacji i wysłać powiadomienie do właściwych osób odpowiedzialnych za obsługę incydentów.
Kryteria poprawności	System DLP wykrył i zablokował wyciek informacji. System DLP wysłał powiadomienie o zdarzeniu do właściwych osób.

Załącznik C. Definicja przypadków testowych dla modułu zarządzania

Identyfikator przypadku testowego	PT_DLP_M-01
Opis przypadku testowego	Powiązanie nazwy użytkownika w domenie Active Directory z incydentem związanym z wyciekiem informacji, zidentyfikowanym przez system DLP.
Zbiór wartości wejściowych	Wartości wejściowe określone w innych przypadkach scenariusza.
Warunki wykonania	Działający system DLP. Integracja z kontrolerem domeny Active Directory. Podejmowane są działania z innych przypadków testowych.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji i podjąć działanie właściwe dla danego zdarzenia. System DLP powinien powiązać zaistniałe zdarzenie z nazwą użytkownika, który wykonał działanie niezgodne z przyjętą polityką.
Kryteria poprawności	System DLP powiązał wykryte zdarzenie z nazwą użytkownika.

Identyfikator przypadku testowego	PT_DLP_M-02
Opis przypadku testowego	Integracja systemu DLP z systemem zarządzania informacjami i zdarzeniami bezpieczeństwa, polegająca na przesłaniu informacji z systemu DLP do systemu SIEM – ArcSight i uwzględnienia ich w procesie korelacji.
Zbiór wartości wejściowych	Wartości wejściowe określone w innych przypadkach scenariusza.
Warunki wykonania	Działający system DLP. Integracja systemu DLP z systemem SIEM. Podejmowane są działania z innych przypadków testowych.
Opis czynności	*<do uzupełnienia na etapie wdrożenia systemu DLP>*
Oczekiwane wyniki	System DLP powinien wykryć próbę wykonania nieautoryzowanej operacji i podjąć działanie właściwe dla danego zdarzenia. System DLP przesyła informacje o zarejestrowanym zdarzeniu do systemu SIEM.
Kryteria poprawności	System DLP przesłał informację o zdarzeniu do systemu SIEM.

PROTOKÓŁ ODBIORU WYKONANIA TESTÓW

Opis czynności	Potwierdzenie wykonania etapu testu	Uwagi
Utworzenie sygnatur plików podlegających ochronie.		Zamawiający przygotuje i wskaże zasób sieciowy (serwer plików) z plikami, które będą podlegać ochronie.
Przygotowanie i przetestowanie polityki korzystającej z danych utworzonych w poprzednim zadaniu, która wykrywa i blokuje informacje chronione przesyłane w sieci (poczta, www) i kopiowane na zewnętrzne nośniki danych (USB, FireWire, CD/DVD).		Testy powinny wykazać, że system skutecznie wykrywa i blokuje informacje chronione przed wyciekiem. Zamawiający wskaże zakresy danych przesyłanych przez sieć czy kopiowanych na zewnętrzne nośniki.
Przygotowanie i przetestowanie polityki korzystającej z wyrażeń regularnych i słów kluczowych, która wykrywa i blokuje informacje przesyłane w sieci (poczta, www) i kopiowane na zewnętrzne nośniki danych (USB, FireWire, CD/DVD)		Test powinny wykazać, że system skutecznie wykrywa i blokuje informacje chronione przed wyciekiem oraz nie generuje fałszywych alarmów. Zamawiający wskaże słowa kluczowe i wzorce danych (np. PESEL).
Przetestowanie polityki wykrywającej dane chronione znajdujące się na lokalnych dyskach stacji roboczej.		Testy powinny wykazać, że agent nie obciąża procesora oraz pamięci a jego praca nie wpływa negatywnie na działanie stacji roboczej. Testy powinny również wykazać, że agent skutecznie rozpoznaje dane chronione znajdujące się w plikach o formatach excel, doc, xml, inne.
Powiadamianie poprzez wiadomość email w języku polskim użytkownika o incydencie (dotyczy modułu sieciowego) oraz powiadamianie poprzez komunikat w języku polskim na konsoli (dotyczy		Testy powinny wykazać, że system umożliwia automatycznie przesyłanie wiadomości email i umożliwia

modułu na stacje robocze).		wyświetlanie komunikatów (okno pop-up) na stacji roboczej.
Blokowanie prób przesłania chronionych informacji za pomocą aplikacji zainstalowanych na stacji roboczej.		Testy powinny wykazać, że agent na stacji roboczej skutecznie blokuje próby przesyłania chronionych informacji. Testy powinny również wykazać, że agent nie generuje fałszywych alarmów podczas pracy użytkowników.

..... **…….**

podpis i pieczęć Zamawiającego **podpis i pieczęć Wykonawcy**

ZAŁĄCZNIK NR 11 DO SPECYFIKACJI
(po podpisaniu umowy stanie się załącznikiem nr 6 do umowy)

SZCZEGÓŁOWA SPECYFIKACJA CENOWO - SPRZĘTOWA

Część A* pozycje wypełnia Wykonawca w zależności od zaoferowanej konfiguracji
Oświadczenie o poszczególnych cenach jednostkowych, zaoferowanym sprzęcie oraz licencjach

Lp	**Sprzęt oraz licencje**	**Oznaczenie produktu** Wykonawca zobowiązany jest podać dane oferowanego produktu/produktów (producent, model, typ, wersja), w tym rodzaj licencji	**Cena jednostkowa netto (zł)**	**Ilość**	Cena łączna netto (zł)	**Podatek VAT (zł)**	**Cena łączna brutto (zł)**
1							
2							
3							
4							
5							
6							
7							
8							
9							
10**							
				RAZEM			

Część B

Wynagrodzenie za konfigurację, integrację i wdrożenie, obejmujące autorskie prawa majątkowe do wszelkich składników systemu do ochrony przed wyciekiem informacji

cena netto .....,..... zł

(słownie:.....)

podatek od towarów i usług VAT – .....,..... zł

(słownie: .....)

cena brutto .....,..... zł

(słownie:.....)

Część C

Wynagrodzenie za świadczenie powdrożeniowych usług gwarancyjnych, konserwacyjnych, serwisowych i nadzoru autorskiego

cena netto .....,..... zł

(słownie:.....)

podatek od towarów i usług VAT – .....,..... zł

(słownie: .....)

cena brutto .....,..... zł

(słownie:.....)

Wartość kwartalna netto	**Wartość kwartalna brutto**	**Przewidywana liczba kwartałów na jaką zostanie podpisana umowa**	**Wartość brutto w okresie obowiązywania umowy** ***(2x3)***
1	2	3	4
		8	

.....

Podpis i pieczęć Wykonawcy