Wojewódzki Inspektorat Weterynarii z siedzibą w Siedlcach, ul. Kazimierzowska 29, 08-110 Siedlce.

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA (SIWZ)

w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie przetargu nieograniczonego dla dostaw o wartości zamówienia poniżej równowartości kwoty 144.000 EURO.

Przedmiot zamówienia:

Dostawa oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach.

Zatwierdził:

_____

(pieczęć i podpis)

Siedlce 2019 r.

ROZDZIAŁ I – POSTANOWIENIA OGÓLNE.

1. **Nazwa oraz adres Zamawiającego:**
   Wojewódzki Inspektorat Weterynarii z siedzibą w Siedlcach
   08-110 Siedlce
   ul. Kazimierzowska 29
   NIP: 821-20-68-188
   telefon: + 48 (25) 63 264 59
   adres strony internetowej: **www.wiw.mazowsze.pl**

2. **Oznaczenie postępowania.**
   Postępowanie, którego dotyczy niniejsza SIWZ oznaczone jest znakiem: **WIW-AD.272.97.2019.** Wykonawcy zobowiązani są do powoływania się na wyżej podane oznaczenie we wszelkich kontaktach z Zamawiającym.

3. **Tryb udzielenia zamówienia, procedura.**

   3.1. Postępowanie o udzielenie zamówienia prowadzone jest w trybie przetargu nieograniczonego o wartości szacunkowej poniżej 144.000 EURO na podstawie ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2018 r., poz. 1986, z późn. zm.).

   3.2. Procedura z art. 24aa ust. 1 ustawy tzw. „procedura odwrócona" - Zamawiający informuje, że stosownie do możliwości jakie daje art. 24aa ust. 1 ustawy najpierw dokona oceny ofert, a następnie zbada czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

   3.3. Ilekroć w niniejszej SIWZ zastosowane jest pojęcie „**ustawa**", „**ustawa Pzp**" lub „**Pzp**", należy przez to rozumieć ustawę Prawo zamówień publicznych, o której mowa w pkt. 3.1.

   3.4. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej, o której mowa w art. 91a - 91c ustawy Pzp.

4. **Opis przedmiotu zamówienia.**

   4.1. Przedmiotem zamówienia jest **dostawa oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach.**

   4.2. Szczegółowe określenie zakresu przedmiotu zamówienia zawarte jest w Rozdziale XVI SIWZ: „Szczegółowy opis przedmiotu zamówienia".

   4.3. Zamawiający nie przewiduje zawarcia umowy ramowej.

   4.4. Klasyfikacja wg Wspólnego Słownika zamówień:
   a) **Pakiet 1**: 30232110-8 drukarki laserowe, 30121100-4 - fotokopiarki,,
   b) **Pakiet 2**: 48219000-6 - Pakiety oprogramowania do różnych operacji sieciowych,
   c) **Pakiet 3**: 30233141-1 - Pamięci do przechowywania danych, 30234500-3 - nadmiarowa macierz niezależnych dysków RAID,
   d) **Pakiet 4**: 32422000-7 - Elementy składowe sieci, 30216130-6 - czytniki kodu kreskowego, 30237220-7 - podkładki pod myszy,
   e) **Pakiet 5**: 30237280-5 - Urządzenia zasilające,
   f) **Pakiet 6:** 32413100-2 Routery sieciowe.

4.5. Zamawiający nie dopuszcza składania ofert wariantowych w rozumieniu art. 2 pkt 7 ustawy Pzp.
4.6. Zamawiający dopuszcza składanie ofert częściowych w rozumieniu art. 2 pkt 6 ustawy Pzp. Najmniejszą częścią jest Pakiet, jak niżej:
4.6.1. **Pakiet 1: Dostawa urządzeń wielofunkcyjnych,**
4.6.2. **Pakiet 2: Dostawa oprogramowania do kompleksowego zarządzania zasobami IT,**
4.6.3. **Pakiet 3: Dostawa urządzenia – serwer NAS z dyskami,**
4.6.4. **Pakiet 4: Dostawa akcesoriów komputerowych,**
4.6.5. **Pakiet 5: Dostawa zasilaczy awaryjnych – UPS,**
4.6.6. **Pakiet 6: Dostawa urządzeń firewall.**
4.7. Zamawiający nie przewiduje zamówień uzupełniających.
4.8. Zamawiający nie przewiduje rozliczenia w walucie obcej.
4.9. Zamawiający nie przewiduje zmian cen wynikających ze zmiany kursów walut.

5. **Termin wykonania i miejsce realizacji zamówienia.**

5.1. Termin realizacji zamówienia: Zgodnie z harmonogramem dostaw stanowiącym **Załącznik nr 6 do SIWZ.**

ROZDZIAŁ II - WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ PODSTAWY WYKLUCZENIA Z POSTĘPOWANIA.

1. W postępowaniu mogą brać udział Wykonawcy, którzy nie podlegają wykluczeniu z postępowania o udzielenie zamówienia w okolicznościach, o których mowa w art. 24 ust. 1 pkt 12-23 PZP.
2. W postępowaniu mogą brać udział Wykonawcy, którzy spełniają warunki udziału w postępowaniu, o których mowa w art. 22 ust. 1 PZP dotyczące:
   2.1. w zakresie kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów – Zamawiający nie stawia szczególnych wymagań w zakresie opisu spełniania tego warunku udziału w postępowaniu.
   2.2. w zakresie sytuacji ekonomicznej lub finansowej – Zamawiający nie stawia szczególnych wymagań w zakresie opisu spełniania tego warunku udziału w postępowaniu.
   2.3. w zakresie zdolności technicznej lub zawodowej – Zamawiający nie stawia szczególnych wymagań w zakresie opisu spełniania tego warunku udziału w postępowaniu.
3. Ocena spełniania warunków udziału w postępowaniu dokonana zostanie zgodnie z formułą „spełnia”/„nie spełnia”, w oparciu o informacje zawarte w dokumentach lub oświadczeniach złożonych przez Wykonawców.
4. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia, każdy z warunków udziału w postępowaniu określonych w pkt 2 winien spełniać co najmniej jeden z tych wykonawców albo wszyscy ci Wykonawcy wspólnie. Żaden z wykonawców wspólnie ubiegających się o udzielenie zamówienia nie może podlegać wykluczeniu z postępowania.
5. Na podstawie art. 22d ust. 2 PZP Zamawiający może, na każdym etapie postępowania, uznać, że wykonawca nie posiada wymaganych zdolności, jeżeli zaangażowanie zasobów technicznych lub zawodowych wykonawcy w inne przedsięwzięcia gospodarcze wykonawcy może mieć negatywny wpływ na realizację zamówienia.

ROZDZIAŁ III - WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW, JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA BRAKU PODSTAW DO WYKLUCZENIA Z POSTĘPOWANIA ORAZ W CELU POTWIERDZENIA SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU.

1. W celu potwierdzenia braku podstaw do wykluczenia z postępowania, o których mowa w Rozdziale II pkt 1 oraz w celu potwierdzenia spełniania warunków udziału w postępowaniu, Wykonawca będzie obowiązany przedstawić Zamawiającemu następujące oświadczenia i dokumenty (w terminach wskazanych w niniejszej SIWZ):
   1.1. Aktualne na dzień składania ofert Oświadczenie wykonawcy zwane dalej „Oświadczeniem", którego wzór określa załącznik nr 1 do SIWZ, stanowiące wstępne potwierdzenie, że wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.
   1.2. Odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 PZP.
2. Dokument wskazany w pkt 1.2 Wykonawca będzie obowiązany złożyć w terminie wskazanym przez Zamawiającego, nie krótszym niż 5 dni, określonym w wezwaniu wystosowanym przez Zamawiającego do Wykonawcy po otwarciu ofert.
3. Dokument wskazany w pkt 1.1 należy dołączyć do oferty.
4. W celu potwierdzenia braku podstaw do wykluczenia z postępowania o udzielenie zamówienia w okolicznościach, o których mowa w art. 24 ust. 1 pkt 23 PZP Wykonawca będzie zobowiązany złożyć oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej (wg wzoru stanowiącego **Załącznik nr 2** do SIWZ). Niezwłocznie po otwarciu ofert zamawiający zamieści na stronie internetowej informacje dotyczące: (1) kwoty jaką zamierza przeznaczyć na sfinansowanie zamówienia, (2) firm oraz adresów wykonawców, którzy złożyli oferty w terminie oraz (3) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach. Wykonawca, w terminie 3 dni od dnia zamieszczenia na stronie internetowej ww. informacji przekazuje zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej. Wzór oświadczenia zawarty jest w **Załączniku nr 2** do SIWZ. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dokumenty bądź informacje, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia oświadczenie składa każdy z takich wykonawców.
5. Wykonawca może polegać na zdolnościach technicznych lub innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków. Wykonawca w takiej sytuacji musi udowodnić zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia. Dokument, z którego będzie wynikać zobowiązanie podmiotu trzeciego powinien wyrażać w sposób jednoznaczny wolę udostępnienia Wykonawcy ubiegającemu się o zamówienie, odpowiedniego zasobu, czyli wskazywać jakiego zasobu dotyczy, określać jego rodzaj, zakres, czas udostępnienia oraz inne okoliczności wynikające ze specyfiki danego zasobu.

6. Jeżeli Wykonawca, wykazując spełnianie warunków, o których mowa w art. 22 ust. 1b PZP, polega na zasobach innych podmiotów na zasadach określonych w art. 22a ust. 1 PZP, Wykonawca będzie zobowiązany do:
   6.1. złożenia oświadczenia podmiotu trzeciego o spełnieniu warunków udziału w postępowaniu (w zakresie warunku, w stosunku do którego udostępnia swój potencjał) i braku podstaw do wykluczenia.
   6.2. przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w Rozdziale III pkt 1.2. Dokumenty wymienione w Rozdziale III pkt 1.2 Wykonawca będzie obowiązany złożyć w terminie wskazanym przez Zamawiającego, nie krótszym niż 5 dni, określonym w wezwaniu wystosowanym przez Zamawiającego do Wykonawcy po otwarciu ofert.
7. W przypadku oferty wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum):
   7.1. w formularzu oferty należy wskazać firmy (nazwy) wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia;
   7.2. oferta musi być podpisana w taki sposób, by wiązała prawnie wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia. Osoba podpisująca ofertę musi posiadać umocowanie prawne do reprezentacji. Umocowanie musi wynikać z treści pełnomocnictwa załączonego do oferty – treść pełnomocnictwa powinna dokładnie określać zakres umocowania;
   7.3. „Oświadczenie", którego wzór określa **Załącznik nr 1** do SIWZ składa każdy z wykonawców wspólnie ubiegających się o zamówienie.
   7.4. dokumenty, o których mowa w Rozdziale III pkt od 1.2 obowiązany będzie złożyć każdy z wykonawców wspólnie ubiegających się o udzielenie zamówienia.
   7.5. wszyscy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia będą ponosić odpowiedzialność solidarną za wykonanie umowy;
   7.6. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia wyznaczą spośród siebie Wykonawcę kierującego (lidera), upoważnionego do zaciągania zobowiązań, otrzymywania poleceń oraz instrukcji dla i w imieniu każdego, jak też dla wszystkich partnerów;
   7.7. Zamawiający może w ramach odpowiedzialności solidarnej żądać wykonania umowy w całości przez lidera lub od wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia łącznie lub każdego z osobna.
8. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, zamawiający może na każdym etapie postępowania wezwać wykonawców do złożenia wszystkich lub niektórych oświadczeń lub dokumentów potwierdzających, że nie podlegają wykluczeniu i spełniają warunki udziału w postępowaniu, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio oświadczenia lub dokumenty nie są już aktualne, do złożenia aktualnych oświadczeń lub dokumentów.
9. Ponadto Zamawiający żąda od Wykonawcy złożenia wraz z ofertą pełnomocnictwa udzielanego osobom podpisującym ofertę, o ile prawo do reprezentowania Wykonawcy w powyższym zakresie nie wynika wprost z dokumentu rejestrowego. Treść pełnomocnictwa musi jednoznacznie określać czynności, co do wykonywania, których pełnomocnik jest upoważniony. Pełnomocnictwo musi być przedstawione w formie oryginału, poświadczonej notarialnie za zgodność z oryginałem kopii, sporządzonego przez notariusza

odpisu lub wyciągu z dokumentu, lub kopii poświadczonej za zgodność z oryginałem przez mocodawcę.

ROZDZIAŁ IV - WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW SKŁADANYCH PRZEZ WYKONAWCĘ W POSTĘPOWANIU W CELU POTWIERDZENIA OKOLICZNOŚCI, O KTÓRYCH MOWA W ART. 25 UST. 1 PKT 2 USTAWY PZP.

1. Wykonawca na potwierdzenie spełniania przez oferowany przedmiot zamówienia wymagań określonych przez zamawiającego o których mowa w Rozdziale XVI, składa:
   1.1 Specyfikację oferowanego przedmiotu zamówienia na formularzu zgodnym z treścią **Załącznika nr 5** do SIWZ (w zakresie którego dotyczy oferta).
2. Dokument wskazany w pkt 1.1 Wykonawca będzie obowiązany złożyć do oferty w postaci oryginału.

ROZDZIAŁ V - INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJACEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIE Z WYKONAWCAMI.

1. W przedmiotowym postępowaniu składanie ofert oraz oświadczeń przez Wykonawcę odbywa się za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. z 2018 r. poz. 2188, z późn. zm.), osobiście lub za pośrednictwem posłańca na adres: tj. Wojewódzki Inspektorat Weterynarii z siedzibą w Siedlcach, ul. Kazimierzowska 29; 08-110 Siedlce, w Kancelarii Zamawiającego w godzinach urzędowania, tj.: od poniedziałku do piątku w godzinach od 8.15 do 16.15.
2. Oświadczenia lub dokumenty składane przez Wykonawcę w postępowaniu na wezwanie Zamawiającego zgodnie z art. 26 ustawy mogą być przesłane Zamawiającemu w wersji elektronicznej (skany dokumentów) drogą elektroniczną, a następnie niezwłocznie przesłane w formie pisemnej za pośrednictwem operatora osobiście lub za pośrednictwem posłańca.
3. Komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie pytań, wyjaśnień wniosków, zawiadomień oraz innych informacji obywać się będzie przy użyciu poczty elektronicznej na adres: zamowienia@wiw.mazowsze.pl
4. Osobą uprawnioną do porozumiewania się z Wykonawcami w związku z toczącym się postępowaniem jest: Łukasz Majewski, telefon: + 48 (25) 63 264 59 wew. 36.
5. Fakt otrzymania wniosków, zawiadomień i informacji przesłanych przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2019r. poz. 123, z późn. zm.) należy niezwłocznie potwierdzić tą samą drogą.
6. W przypadku braku potwierdzenia otrzymania wiadomości przez Wykonawcę, Zamawiający domniema, iż pismo wysłane przez Zamawiającego na adres poczty elektronicznej podany przez Wykonawcę zostało mu doręczone w sposób umożliwiający zapoznanie się Wykonawcy z treścią pisma.

ROZDZIAŁ VI - WYMAGANIA DOTYCZĄCE WADIUM.

1. Zamawiający w przedmiotowym postępowaniu nie żąda wniesienia wadium.

ROZDZIAŁ VII - TERMIN ZWIĄZANIA OFERTĄ.

1. Termin związania ofertą wynosi 30 dni.
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
3. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania z ofertą na czas niezbędny do zawarcia umowy w sprawie zamówienia publicznego, 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.
4. W przypadku wniesienia odwołania po upływie terminu składania ofert bieg terminu związania z ofertą ulega zawieszeniu do czasu ogłoszenia przez Izbę orzeczenia.

ROZDZIAŁ VIII - OPIS SPOSOBU PRZYGOTOWANIA OFERT

1. Każdy Wykonawca zobowiązany jest zapoznać się dokładnie z informacjami zawartymi w SIWZ i przygotować ofertę zgodnie z wymaganiami Zamawiającego.
2. Wykonawca na etapie przygotowywania oferty powinien zweryfikować dostępność wyspecyfikowanych przez Zamawiającego produktów oraz możliwość ich dostarczenia w określonym przez Zamawiającego terminie.
3. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ. Wyjaśnienia treści SIWZ udzielane będą przez Zamawiającego z zachowaniem zasad określonych w art. 38 ustawy Pzp.
4. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Wnioski, które Zamawiający otrzyma po tym terminie, mogą pozostać bez odpowiedzi.
5. Treść wszystkich pytań o wyjaśnienie treści SIWZ i udzielonych odpowiedzi, Zamawiający przekaże za pośrednictwem poczty elektronicznej wszystkim, którym SIWZ została przekazana, bez ujawniania źródła zapytania oraz umieści je na stronie internetowej.
6. W uzasadnionych przypadkach Zamawiający może przed terminem składania ofert zmienić treść specyfikacji istotnych warunków zamówienia. Dokonaną zmianę treści specyfikacji Zamawiający udostępni na stronie internetowej.
7. Ofertę należy sporządzić w formie pisemnej, w języku polskim. Zaleca się, aby oferta była napisana na komputerze, maszynie do pisania lub w sposób czytelny - ręcznie długopisem bądź niezmywalnym atramentem. Wszelkie dokumenty i oświadczenia w językach obcych należy złożyć wraz z tłumaczeniem na język polski. Wszelkie poprawki lub zmiany dokonane w

treści oferty (przed jej złożeniem) muszą być parafowane przez osobę (osoby) podpisującą ofertę.

8. Oferta i wszystkie załączone dokumenty i oświadczenia składane przez Wykonawcę muszą być podpisane czytelnie lub opatrzone dodatkowo pieczątkami imiennymi przez osoby zdolne do czynności prawnych w imieniu Wykonawcy i zaciągania w jego imieniu zobowiązań finansowych, w wysokości odpowiadającej cenie oferty (Wykonawców wspólnie ubiegających się o udzielenie zamówienia). Oznacza to, że jeżeli z dokumentu(ów) określającego(ych) status prawny Wykonawcy(ów) lub pełnomocnictwa (pełnomocnictw) wynika, że do reprezentowania Wykonawcy(ów) upoważnionych jest łącznie kilka osób, dokumenty wchodzące w skład oferty muszą być podpisane przez wszystkie te osoby.
9. O ile upoważnienie nie wynika z dokumentów rejestrowych w przypadku podpisania oferty przez pełnomocnika, do oferty należy dołączyć oryginał lub poświadczoną za zgodność z oryginałem przez notariusza, kopię pełnomocnictwa wystawionego na reprezentanta Wykonawcy przez osoby do tego umocowane.
10. Zamawiający zaleca, aby wszystkie strony oferty wraz z załącznikami były jednoznacznie ponumerowane i złączone w sposób uniemożliwiający ich zdekompletowanie.
11. Wykonawca może złożyć w postępowaniu tylko jedną ofertę.
12. Kopia dokumentu wymaga zapisu „za zgodność z oryginałem" lub innego równoznacznego zapisu.
13. Zamawiający może żądać przedstawienia oryginału lub notarialnie poświadczonej kopii dokumentu wyłącznie wtedy, gdy złożona przez Wykonawcę kopia dokumentu jest nieczytelna lub budzi wątpliwości, co do jej prawdziwości.
14. Wszelkie koszty związane ze sporządzeniem oferty oraz jej złożeniem ponosi Wykonawca, niezależnie od wyniku postępowania, z zastrzeżeniem art. 93 ust. 4 ustawy Pzp.
15. Wykonawca może przed upływem terminu do składania ofert, zmienić lub wycofać ofertę.
16. Wykonawca może wprowadzić zmiany, poprawki, modyfikacje i uzupełnienia do złożonej oferty pod warunkiem, że Zamawiający otrzyma pisemne zawiadomienie o wprowadzeniu zmian przed terminem składania ofert. Powiadomienie o wprowadzeniu zmian musi być złożone według takich samych zasad, jak składana oferta tj. w kopercie odpowiednio oznakowanej napisem ,,ZMIANA". Koperty oznaczone ,,ZMIANA" zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian, zostaną dołączone do oferty.
17. Żadna oferta nie może być modyfikowana lub wycofana po upływie terminu składania ofert**.**
18. Ofertę wraz z wszystkimi załącznikami należy umieścić w kopercie, trwale zaklejonej, odpowiednio zabezpieczonej przed uszkodzeniem w czasie transportu, oznakowanej w następujący sposób:

Wojewódzki Inspektorat Weterynarii z siedzibą w Siedlcach
ul. Kazimierzowska 29, 08-110 Siedlce.
(nazwa i adres Zamawiającego)

oraz opisane:

Dostawa oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach – Pakiet nr ...

WIW-AD.272.97.2019
(nazwa zamówienia)

Nie otwierać przed dniem: 6 grudnia 2019 roku; godz.: 9:00.

19. W przypadku, gdyby oferta zawierała informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2019 r., poz. 1010), Wykonawca winien w sposób niebudzący wątpliwości zastrzec, które informacje stanowią tajemnicę przedsiębiorstwa i nie mogą być udostępniane. Informacje te – powinny być opatrzone klauzulą: „nie udostępniać innym uczestnikom postępowania, informacje stanowią tajemnicę przedsiębiorstwa i umieszczone w osobnym wewnętrznym opakowaniu (tj. w odrębnej kopercie oznakowanej literką „B") trwale ze sobą połączone i ponumerowane. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust.4 ustawy Pzp.
20. Zawartość oferty: Wykonawca winien złożyć w terminie wskazanym w Rozdziale IX SIWZ:
    20.1. Wypełniony, podpisany przez osobę/y uprawnioną/e do reprezentowania Wykonawcy formularz oferty przetargowej, stanowiący **Załącznik nr 3** do SIWZ.
    20.2. Oświadczenie o niepodleganiu wykluczeniu oraz spełnieniu warunków udziału w postępowaniu - **Załącznik nr 1** do SIWZ.
    20.3. Pełnomocnictwo udzielane osobom podpisującym ofertę, o ile prawo do reprezentowania Wykonawcy w powyższym zakresie nie wynika wprost z dokumentu rejestrowego. Treść pełnomocnictwa musi jednoznacznie określać czynności, co do wykonywania, których pełnomocnik jest upoważniony. Pełnomocnictwo musi być przedstawione w formie oryginału, poświadczonej notarialnie za zgodność z oryginałem kopii, sporządzonego przez notariusza odpisu lub wyciągu z dokumentu, lub kopii poświadczonej za zgodność z oryginałem przez mocodawcę.
    20.4. Specyfikację oferowanego przedmiotu zamówienia na formularzu zgodnym z treścią **Załącznika nr 5** do SIWZ.

ROZDZIAŁ IX - MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

1. Oferty winny być złożone w siedzibie Zamawiającego tj. **Wojewódzki Inspektorat Weterynarii z siedzibą w Siedlcach, ul. Kazimierzowska 29; 08-110 Siedlce, w kancelarii**, w terminie do dnia **6 grudnia 2019 r. do godziny 8:30.**

2. Oferty, które zostały złożone po terminie określonym w ust. 1 zostaną zwrócone wykonawcom niezwłocznie.
3. Oferty zostaną otwarte w siedzibie Zamawiającego tj. **Wojewódzki Inspektorat Weterynarii z siedzibą w Siedlcach, ul. Kazimierzowska 29; 08-110 Siedlce, w zespole ds. administracyjnych**, w dniu **6 grudnia 2019r.** o godzinie **9:00.**
4. Otwarcie ofert jest jawne. Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia. Podczas otwarcia ofert podane zostaną nazwy (firmy) oraz adresy wykonawców, a także informacje dotyczące ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

ROZDZIAŁ X – OPIS SPOSOBU OBLICZENIA CENY OFERTY.

1. Cena oferty będzie obejmować całkowity koszt wykonania zamówienia oraz wszelkie koszty związane z wykonaniem zamówienia, o którym mowa w Rozdziale XVI SIWZ „Opis przedmiotu zamówienia" oraz w Załączniku nr 4 do SIWZ „Wzór umowy", oraz wszelkie inne ewentualne obciążenia, w szczególności podatek VAT oraz ewentualne cło.
2. Wykonawca określi cenę w złotych polskich.
3. Ceny muszą być podane **z dokładnością do setnych części złotego.**
4. Ceny netto dostawy (bez VAT) należy przemnożyć przez ilość oferowanych jednostek miary i wyliczyć wartość dostawy netto (bez VAT). Do wartości dostawy netto (bez VAT) Wykonawca doliczy podatek VAT w obowiązującej wysokości, i w ten sposób wyliczy wartość dostawy brutto (z VAT).
5. Jeżeli Wykonawca nie będzie zobowiązany zgodnie z przepisami prawa polskiego do naliczenia VAT od wartości dokonywanej dostawy, a obowiązek zapłaty tego podatku (i ewentualnie cła) będzie obciążał Zamawiającego, wówczas do podanych przez takiego Wykonawcę wartości dostawy netto (bez VAT) dla poszczególnych Pozycji Zamawiający doliczy - dla potrzeb porównania i oceny ofert - kwotę VAT (i ewentualnie cła) w obowiązującej Zamawiającego wysokości, następnie zsumuje uzyskane wartości, i tak uzyskaną cenę oferty porówna z cenami brutto pozostałych ofert.
6. W przypadku, gdy w wyniku wyboru najkorzystniejszej oferty obowiązek zapłaty podatku VAT (i ewentualnie cła) będzie ciążył na Zamawiającym, wynagrodzeniem Wykonawcy będzie kwota bez podatku VAT (i ewentualnie cła).
7. Ceny jednostkowe dostawy netto (bez VAT) określone przez Wykonawcę będą stanowiły podstawę do rozliczeń w całym okresie trwania umowy.
8. Ceny jednostkowe dostawy netto (bez VAT) nie będą podlegać waloryzacji.

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

1. Zamawiający za najkorzystniejszą uzna ofertę niepodlegającą odrzuceniu, która uzyska największą liczbę punktów obliczona w oparciu o podane kryteria oceny ofert.

2. Zamawiający dokona oceny ofert według następujących kryteriów i ich wag:
   - **CENA o wadze 60% (C)**
   - **TERMIN PŁATNOŚCI o wadze 40% (TP)**
3. W kryterium **„CENA”** ocena ofert zostanie dokonana przy zastosowaniu wzoru:

$$\textbf{CENA (C)} = \frac{\textbf{CN}}{\textbf{COB}} \textbf{ x 60}$$

gdzie:
C - liczba punktów przyznanych wykonawcy za cenę.
CN – najniższa cena spośród zaoferowanych ofert.
COB - cena ocenianej oferty.

4. W kryterium **„TERMIN PŁATNOŚCI”** ocena ofert zostanie dokonana przy zastosowaniu wzoru:

$$\textbf{TERMIN PŁATNOŚCI (TP)} = \textbf{[(TPOO-21):(NTP-21)] x 40}$$

gdzie:
TP - liczba punktów przyznanych wykonawcy za zaoferowany termin płatności.
TPOO - termin płatności (w dniach) oferty ocenianej.
NTP - najdłuższy termin płatności (w dniach) spośród ocenianych ofert.

Uwaga: zaoferowany termin płatności nie może być krótszy niż 21 dni oraz dłuższy niż 30 dni od dnia otrzymania przez Zamawiającego faktury VAT.
Zamawiający wyjaśnia, iż punkty w tym kryterium oceny ofert będzie przyznawał na podstawie oświadczenia Wykonawcy zawartego w treści oferty (**Załącznik nr 3 do SIWZ pkt 6**).

5. Wykonawca, składając ofertę, ma obowiązek poinformować Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
   Jeżeli złożono ofertę, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny (wykonawca podaje jedynie wartość netto) podatek od towarów i usług.
   Wartość podatku VAT płaconego przez zamawiającego zostanie doliczona do podanej przez Wykonawcę wartości netto (powstaje u Zamawiającego obowiązek podatkowy) w przypadku:
   a) wewnątrzwspólnotowego nabycia towarów,
   b) mechanizmu odwróconego obciążenia, w odniesieniu do wprowadzonych już, jak i wprowadzonych przedmiotową nowelizacją zmian w ustawie o VAT,

c) importu usług lub importu towarów, z którymi wiąże się analogiczny obowiązek doliczenia przez Zamawiającego przy porównywaniu cen ofertowych podatku VAT.

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

1. Wykonawca, którego ofertę wybrano jako najkorzystniejszą jest obowiązany do zawarcia umowy w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni - jeżeli zostało przesłane w inny sposób.
2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminów, o których mowa powyżej, jeżeli w postępowaniu o udzielenie zamówienia została złożona tylko jedna oferta.
3. W przypadku poinformowania Zamawiającego o niezgodnej z przepisami ustawy czynności podjętej przez niego lub zaniechaniu czynności do której był zobowiązany oraz w przypadku wniesienia odwołania - po wyborze najkorzystniejszej oferty, Zamawiający wyznaczy nowy termin podpisania umowy. Niedopełnienie przez Wykonawcę tego terminu, zostanie poczytane przez Zamawiającego jako uchylanie się Wykonawcy od podpisania umowy.
4. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający zastrzega sobie prawo żądania, przed podpisaniem umowy w sprawie udzielenia zamówienia publicznego, umowy regulującej współpracę tych wykonawców.

ROZDZIAŁ XIII - WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY.

Zamawiający nie wymaga zabezpieczenia należytego wykonania umowy.

ROZDZIAŁ XIV - ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO. WZÓR UMOWY. ZMIANY UMOWY.

1. Postanowienia umowy określa wzór umowy stanowiący **Załącznik nr 4 do SIWZ**.
2. Wykonawca, który przedstawił najkorzystniejszą ofertę pod względem kryteriów oceny ofert zamówienia, będzie zobowiązany do podpisania w siedzibie Zamawiającego umowy zgodnej ze wzorem umowy załączonym do SIWZ.
3. Do przedstawionego wzoru umowy zostaną wprowadzone zobowiązania Wykonawcy w trakcie procedury, wynikające z przedstawionej przez niego oferty.
4. Wzór umowy, po upływie terminu do składania ofert, nie podlega negocjacjom złożenie oferty jest równoznaczne z pełną akceptacją umowy przez Wykonawcę.

5. Dopuszcza się możliwość zmiany umowy w zakresie zmiany obowiązującej stawki podatku VAT w przypadku ustawowej zmiany stawki podatku VAT.

ROZDZIAŁ XV - 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, o których mowa w Dziale VI ustawy Pzp.

ROZDZIAŁ XVI SIWZ – SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest **dostawa oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach** w następujących ilościach i o następujących parametrach technicznych:

Pakiet nr 1: Dostawa urządzeń wielofunkcyjnych

Lp.	Przedmiot zamówienia	Opis - Parametry techniczne	Ilość zamawiana	Wielkość opakowania	Wymagany termin gwarancji
1.	Urządzenie wielofunkcyjne (drukarka/ kopiarka/ skaner)	Urządzenia powinny spełniać poniżej wyspecyfikowane minimalne parametry: 1. Minimalna prędkość wydruku A4/min - 40ppm (BW/kolor); 2. Minimalna prędkość wydruku A3/min 22ppm; 3. Format oryginału - minimum A3; 4. Pamięć RAM minimum - 4 GB; 5. Maksymalny czas uzyskania 1. kopii - BW 4,5 sek., kolor 6.5 sek.; 6. Czas uruchomienia do 22sek.; 7. Minimalna pojemność papieru - 1200 arkuszy; 8. Minimalna pojemność podajnika bocznego - 100 arkuszy; 9. Minimalna ilość źródeł papieru – 3; 10. Wydruk na kopertach z automatycznym podawaniem; 11. Minimalny zakres gramatur papieru od 52 do 300g/m2; 12. Automatyczny druk / kopia dwustronna; 13. Interfejsy: Ethernet (1000BaseT/100Base-TX/10Base-T), USB, bezprzewodowa sieć LAN (IEEE 802.11 b/g/n); 14. Język drukarki: PCL 6, PostScript Level 3; 15. Minimalna pojemność dysku drukarki - 250 GB; 16. Minimalna rozdzielczość kopiowania - 600dpi×600dpi; 17. Minimalna rozdzielczość drukowania - 600dpi×600dpi;	4	szt.	Minimum 36 miesięcy gwarancji producenta urządzenia

		18. Automatyczny dwustronny, jednoprzebiegowy podajnik oryginałów.; 19. Minimalna pojemność podajnika oryginałów: 150 arkuszy; 20. Minimalna prędkość skanowania - 80 stron A4/min jednostronnie; 160 stron A4/min dwustronnie; 21. Skanowanie z wysyłaniem na adresy email, zasoby SMB, zasoby FTP, pamięci USB; 22. Format zapisywanych plików - TIFF, JPEG, PDF, Przeszukiwany PDF, Szyfrowany PDF, XPS, Office Open XML (PowerPoint, Word), PDF/XPX , PDF/A-1b , Sygnatura cyfrowa; 23. Szafka pod urządzenie umożliwiająca postawienie go na podłodze; 24. Czytnik kart zbliżeniowych; 25. System zarzadzania uwierzytelnianiem: W okresie co najmniej 5 lat od dostarczenia urządzeń wykonawca powinien zapewnić działanie jednolitego systemu umożliwiającego logowanie się na urządzeniach za pomocą kart zbliżeniowych. System powinien obsługiwać urządzenia dotychczas znajdujące się w użytkowaniu przez zamawiającego (CANON iRAC 5235i – ilość: 6szt., iRAC 5030i – ilość: 10szt.) 26. Uwierzytelnienie - kontrola funkcji urządzenia (kopiowanie, drukowania, wysyłanie, kolor, druk jednostronny), automatyczne zwalnianie wydruków po zalogowaniu, podgląd wydruku przed zwolnieniem, funkcja wymuszonego wstrzymania wydruku, funkcja wyślij do mnie; 27. Wspólna dla wszystkich maszyn baza użytkowników, nie powinna wymagać zasobów sprzętowych po stronie zamawiającego, jeżeli jest taka konieczność wykonawca dostarczy stosowne zasoby komputerowe. Integracja z AD.			

		28. Raporty użycia z podziałem na urządzenie, użytkownika, grupę, z możliwością zebrania danych z wielu urządzeń. Raport musi zawierać cenę wykonanych prac. 29. System monitorowania urządzeń: Wykonawca powinien zapewnić rozwiązanie pozwalające w okresie co najmniej 5 lat od daty uruchomiania monitorowanie stanu urządzeń z powiadamianiem o : • Małej ilości tonera, błędach, zacięciach papieru, stanie liczników, stopniu zużycia części. • System powinien obsługiwać urządzenia dotychczas znajdujące się w użytkowaniu przez zamawiającego. (CANON iRAC 5235i, iRAC 5030i) 30. Zabezpieczenie dokumentu: • Bezpieczne drukowanie, szyfrowane pliki PDF, podpis urządzenia, zabezpieczające znaki wodne. • Zabezpieczenie danych moduł TPM (Trusted Platform Module), wymazywanie dysku twardego (DoD, minimum 9 razy losowymi danymi), szyfrowanie dysku twardego (FIPS140-2, zatwierdzone); 31. Wydajność czarnego tonera/ów dostarczonego z urządzeniem - min. 60 000 wydruków przy pokryciu 5%; 32. Wydajność kolorowych tonerów dostarczonych z urządzeniem - min. 22 000 wydruków przy pokryciu 5% ; 33. Wydajność bębnów - Min. 125 000 wydruków • Tonery dostarczone z urządzeniem powinny być kompletnym zestawem tonerów tego samego producenta co urządzenie 34. Oferta powinna uwzględniać dostarczenie, instalację urządzeń wraz z konfiguracją (podłączenie do Active Directory) i wygenerowaniem pierwszych wydruków testowych oraz przesłanie skanów na lokalizację sieciową.			

Pakiet 2: Dostawa oprogramowania do kompleksowego zarządzania zasobami IT:

Lp.	Przedmiot zamówienia	Opis - Parametry techniczne	Ilość zamawiana	Wielkość opakowania	Wymagany termin gwarancji
1.	Oprogramowanie do kompleksowego zarządzania zasobami IT	**Oprogramowanie powinno spełniać niżej wyspecyfikowane minimalne parametry:** 1. Oprogramowanie powinno posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Moduły powinny umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. 2. Powinno monitorować infrastrukturę (bezagentowo) obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie (moduł sieciowy): • Serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Mieć możliwość monitorowania czas ich odpowiedzi i procent utraconych pakietów. • Serwerów pocztowych: – monitorować zarówno serwis odbierający, jak i wysyłający pocztę, – możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem), – możliwość wykonywania operacji testowych,	1	oprogramowanie	-

		– możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa. • Monitorowania serwerów WWW i adresów URL. • Obsługi szyfrowania SSL/TLS w powiadomieniach e-mail. • Obsługi urządzeń SNMP wspierających SNMP v1/2/3 (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.). • Obsługi komunikatów syslog i pułapek SNMP. • Monitoringu routerów i przełączników wg: – zmian stanu interfejsów sieciowych, – ruchu sieciowego, – podłączonych stacji roboczych, – ruchu generowanego przez podłączone stacje robocze. • Serwisów Windows: monitor serwisów Windows alarmuje, gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie. • Wydajności systemów Windows: – obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. Program powinien posiadać Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzyć dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). 3. W zakresie inwentaryzacji program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz: a) Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. b) Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.			

		c) Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows, co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. d) Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. e) Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. f) Umożliwiać odczytanie numeru seryjnego (klucze licencyjne). Moduł inwentaryzacji sprzętu powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie: • przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, • definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości – dla danego urządzenia lub oprogramowania powinna istnieć możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX), skan dowolnego dokumentu, czy też własny komentarz; dodatkowo powinna być możliwość importu danych z zewnętrznego źródła (.CSV),			

		• generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania, • archiwizacji i porównywania audytów środków trwałych, • tworzenia kodów kreskowych w Środkach Trwałych, • drukowania kodów kreskowych oraz QR Code (mozaikowe) dla środków trwałych, które posiadają numer inwentarzowy, inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej na system Android. Powinny być dostępne Agenty inwentaryzacji na systemy Android, OS X oraz Linux. Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: a) Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. b) Zarządzanie posiadanymi licencjami. c) Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili powinna istnieć możliwość wykonania aktualnych raportów audytowych. d) Zarządzanie posiadanymi licencjami: raport zgodności licencji. e) Możliwość przypisania do programów numerów seryjnych, wartości itp. Okna audytowe powinny posiadać możliwość filtrowania elementów per oddział. 4. W zakresie obsługi użytkowników program Powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez analizę: • Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),			

		• Monitorowanie procesów (każdy proces - całkowity czas działania oraz czas aktywności użytkownika), • Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona), • Informacji o edytowanych przez użytkownika dokumentach, • Historii pracy (cykliczne zrzuty ekranowe), • Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt), • Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), • Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Możliwość monitorowania kosztów wydruków, • Nagłówków przesyłanej poczty e-mail. Program ponadto powinien posiadać możliwość blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.onet.pl). Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji. 5. Program Powinien umożliwiać realizację zdalnej pomocy użytkownikom. W ramach kontroli stacji użytkownika			

		powinien być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu powinien mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module powinna znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, wpisywane i widoczne dla obu stron. Moduł ten powinien zawierać również komunikator (czat), który umożliwi przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najbardziej typowe problemy. Moduł pomocy zdalnej powinien umożliwić również: • pobieranie listy użytkowników z Active Directory, • przypisywanie pracowników helpdesk do kategorii zgłoszeń, • procesowanie zgłoszeń użytkowników z wiadomości e-mail, • dołączanie załączników do zgłoszeń, • zrzuty ekranowe (podgląd pulpitu), • dystrybucję oprogramowania przez Agenty, • dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), • zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,			

		• możliwość skonfigurowania automatyzacji procesowania zgłoszeń, • planowanie nieobecności pracowników helpdesk, • generowanie raportów obsługi helpdesk 6. Możliwość ochrony danych przed wyciekiem poprzez blokowanie urządzeń. a) Blokowanie urządzeń i nośników danych. b) Możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. c) Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. d) Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. e) Blokownie powinno dotyczyć urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) powinny móc pozostać. Zarządzanie prawami dostępu do urządzeń: a) Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. b) Autoryzowanie urządzeń wskazanych: pendrive'ów, dysków itp. c) Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników lub stacji roboczych. d) Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci lub wybranych stacji roboczych. Audyt operacji na urządzeniach przenośnych: a) Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. b) Podłączenie/odłączenie urządzenia przenośnego.			

		Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. 7. Ochrona przed usunięciem oprogramowania. Program powinien mieć możliwość zabezpieczenia hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet, jeśli użytkownik ma prawa administratora. 8. Program powinien być dostępny w języku polskim. 9. Oferowane oprogramowanie powinno umożliwić w pełni funkcjonalne zarządzanie i monitorowanie minimum 200 urządzeń sieciowych. 10. W ramach dostawy oprogramowania, Wykonawca zobowiązuje się do przeprowadzenia zaawansowanego nieodpłatnego szkolenia technicznego w języku polskim , zapewniającego zdobycie wiedzy niezbędnej do projektowania, wdrażania i optymalizowania rozwiązań wykorzystujących przedmiotowe oprogramowanie a także umiejętność rozwiązywania ewentualnych problemów. Szkolenie powinno odbyć się w centrum treningowym, certyfikowanym przez producenta oprogramowania. Realizacja szkolenia powinna być przeprowadzona według następujących założeń: • Szkolenie powinno być przeprowadzone dla dwóch administratorów systemu Zamawiającego. • Każdy uczestnik szkolenia powinien otrzymać odpowiednie świadectwo (certyfikat) o jego odbyciu. • Szkolenie powinno zostać przeprowadzone przez osoby posiadające odpowiednie kwalifikacje, potwierdzone certyfikatem producenta oprogramowania. • W ramach szkolenia Wykonawca powinien zapewnić szkolonym odpowiednie materiały szkoleniowe, adekwatne do zakresu szkolenia. • Szkolenie powinno zostać przeprowadzone w języku polskim do 14 lutego 2020 w terminie uzgodnionym i zaakceptowanym przez Zamawiającego.			

		11. Dostarczone oprogramowanie powinno zawierać dostawę licencji umożliwiających pełne działanie wszystkich modułów oprogramowania dostępnych w momencie składania oferty oraz pełne zarządzanie minimum 200 urządzeniami sieci ze wsparciem producenta i dostępem do aktualizacji oprogramowania w ciągu 12 miesięcy od dostawy. W ramach oferty Wykonawcy gwarantowane będą określone poniżej warunki: • licencja wieczysta na dostarczone oprogramowanie, • moduł sieciowy dla nielimitowanej ilości monitorowanych urządzeń, • możliwość instalacji wielu konsol administracyjnych, • możliwość przedłużenia Umowy Serwisowej na kolejne 12 miesięcy w cenie nie przekraczającej 20% wartości licencji przy zachowaniu ciągłości usługi, • dostępność oprogramowania w dowolnej konfiguracji modułowej (funkcjonalnej) według rzeczywistych indywidualnych potrzeb użytkownika, • możliwość zwiększenia liczby zarządzanych stacji roboczych w ramach jednej licencji w dowolnym czasie.			

Pakiet 3: Dostawa urządzenia – serwer NAS z dyskami:

Lp.	Przedmiot zamówienia	Opis - Parametry techniczne	Ilość zamawiana	Wielkość opakowania	Wymagany termin gwarancji
1.	Serwer NAS	**Urządzenie powinno spełniać wyspecyfikowane minimalne parametry:** Specyfikacja sprzętowa 1. Obudowa urządzenia wysokości 1U do montażu stelażowego. W komplecie wszystkie elementy montażowe do instalacji w szafie rack 19”. Wskaźniki LED front: HDD 1–4, stan, USB, LAN	1	szt.	Minimum 24 miesiące gwarancji producenta

		2. Procesor czterordzeniowy taktowany zegarem min. 2,0 GHz. Wykonany w architekturze 64-bit x86. Koprocesor arytmetyczny FPU. Wsparcie mechanizmu szyfrowania AES-NI z akceleracją sprzętową. 3. Pamięć systemowa: 4GB SO-DIMM DDR3L (1 x 4GB). Maksymalna pojemność pamięci: 16GB (2 x 8GB). Pamięć flash: 512MB (ochrona systemu operacyjnego przed podwójnym rozruchem) 4. Wnęka dysków: 4 x 3.5-inch SATA 6Gb/s, 3Gb/s Kompatybilność dysków: 3,5-calowe dyski twarde SATA; 2,5-calowe dyski twarde SATA; 2,5-calowe dyski SSD SATA. Możliwa wymiana dysków podczas pracy urządzenia. 5. Port Gigabit sieci Ethernet (RJ45): 4 szt. Port 10 Gigabit sieci Ethernet: 1 x 10GBASE-T (10G/5G/2,5G/1G/100M) - fabrycznie zainstalowana karta PCIe w gnieździe Slot 1: PCIe Gen 2 x4. Obsługa ramek Jumbo. 3 x Port USB 2.0 2 x Port USB 3.0 Opcjonalny Port USB 3.1 Gen 2 (10 Gb/s) na karci rozszerzeń w gnieździe PCIe. 6. Zasilacze nadmiarowe: 2 szt. 250 W, wejście: 110–240 V, 50–60 Hz, 5 A Specyfikacja oprogramowania 7. System operacyjny przygotowany przez producenta urządzenia na bazie LINUX. Obsługiwane systemy operacyjne: Linux i UNIX, Microsoft Windows 7, 8, and 10, Microsoft Windows Server 2003, 2008 R2, 2012, 2012 R2 and 2016. 8. Obsługiwane przeglądarki: Google Chrome, Microsoft Internet Explorer 10 lub nowszy, Mozilla Firefox. 9. Wspierany język interfejsu obsługi systemu operacyjnego: Polski.			

		10. Obsługiwane systemy plików: wewnętrzny zasób dyskowy (EXT4), zewnętrzny zasób dyskowy (EXT3, EXT4, NTFS, FAT32, HFS+, and exFAT) 11. Sieć i przełącznik wirtualny: TCP/IP: Dual stack (IPv4 and IPv6), Jumbo frame (failover, multi-IP settings, port trunking/NIC teaming), DHCP server and client, USB Wi-Fi adapter, Virtual switch WirelessAP Station 12. Zabezpieczenia: Zabezpieczenie dostępu sieciowego z autoblokadą (SSH, Telnet, HTTP(S), FTP, CIFS/SMB, and AFP), Kontrola dostępu udostępnionych folderów (CIFS/SMB), szyfrowanie AES 256-bit woluminów i udostępnionych folderów (FIPS), 256-bit szyfrowanie dysków zewnętrznych (AES), Import i rejestrowanie certyfikatów SSL, natychmiastowe powiadamianie email, SMS, push service, audio, i LCD panel z dwustopniową weryfikacją. 13. Zarządzanie pamięcią masową: • Monitorowanie wykorzystania przestrzeni dyskowej, • Elastyczne woluminy i jednostki LUN z udostępnianiem i odzyskiwaniem przestrzeni, • Obsługiwane typy macierzy RAID: RAID 0, 1, 5, 6, 10, JBOD, Single, • RAID hot spare i globalny hot spare, • Dostosowywanie szybkości odbudowywania macierzy RAID, • Zaawansowane bezpieczne usuwanie danych, • Pule pamięci, • Technologia Qtier (automatyczne tworzenie warstw magazynowych), • Migawki, • Rozszerzenie wolumenu online, • Rozszerzenie puli pamięci online,			

		• Zwiększanie pojemności macierzy RAID online, • Migracja online RAID, • Migracja danych SMART, • Rozszerzenie pamięci za pomocą jednostek rozszerzeń producenta urządzenia, • Roaming w obudowie JBOD • Pamięć podręczna SSD tylko do odczytu lub do odczytu i zapisu • Zły skan bloku i test S.M.A.R.T na dysku twardym. • Odzyskiwanie złych bloków i odzyskiwanie RAID • Obsługa bitmap 14. iSCSI: • iSCSI targets z wieloma jednostkami LUN, • Mapowanie i maskowanie jednostek LUN, • Zwiększenie pojemności jednostek LUN online • Stała rezerwacja SPC-3 15. Zarządzanie energią: • Wake-on-LAN • Tryb gotowości dla dysków wewnętrznych • Zaplanowane włączanie i wyłączanie • Automatyczne włączanie po odzyskaniu zasilania • Obsługa USB i sieciowego UPS z zarządzaniem SNMP 16. Zarządzanie prawami dostępu: • Tworzenie wielu użytkowników • Importowanie i eksportowanie danych użytkownika • Zarządzanie przydziałami użytkowników • Lokalna kontrola dostępu użytkownika (AFP, CIFS / SMB, FTP i WebDAV) 17. Uwierzytelnianie domeny: • Obsługa Microsoft Active Directory (AD) i kontrolera domeny • Serwer i klient LDAP			

		• Logowanie użytkownika domeny (AFP, CIFS / SMB, FTP i File Station) 18. Usługi chmurowe: • Darmowa rejestracja nazwy hosta (DDNS) • Opcjonalne certyfikaty SSL (DDNS) producenta urządzenia • Automatyczna konfiguracja routera za pomocą UPnP • Internetowy menedżer plików z szyfrowaniem HTTPS 2048-bit • CloudLink do zdalnego dostępu bez skomplikowanej konfiguracji routera 19. Usługi synchronizacji: • Synchronizacja plików na wielu urządzeniach z bezpiecznym połączeniem SSL • Selektywna synchronizacja dla określonych folderów lub podfolderów • Foldery zespołu jako centrum plików dla lepszej współpracy Uwaga: Maksymalna liczba zadań synchronizacji wynosi 32. • Udostępnianie plików za pomocą linków e-mail 20. Monitor zasobów: • Monitorowanie zasobów systemu NAS, takich jak procesor, pamięć i sieć • Monitorowanie zasobów pamięci NAS, takich jak woluminy, RAID i aktywność dysku • Monitorowanie wykorzystania zasobów aplikacji NAS • Tworzenie dodatkowej przestrzeni wymiany po zainstalowaniu dysków SSD 21. Wsparcie: • Zgłaszanie problemów zespołowi wsparcia producenta urządzenia z automatycznym gromadzeniem informacji o systemie			

		• Zdalne połączenie między inżynierami wsparcia producenta urządzenia a NAS w celu rozwiązania problemu (za zgodą użytkownika) 22. Administracja sieci: • Zarządzanie systemem z wieloma oknami i wieloma zadaniami • Inteligentny pasek narzędzi i pulpit do wyświetlania statusu systemu • Dynamiczny DNS (DDNS) • Wersje 2 i 3 SNMP • Monitor zasobów • Kosz sieci • Kompleksowe dzienniki (zdarzenia i połączenia) • Serwer i klient Syslog • Tworzenie kopii zapasowych i przywracanie ustawień systemu • Aplikacja mobilna do zdalnego monitorowania i zarządzania systemem 23. Serwer plików: • Udostępnianie plików w systemach Windows, Mac i Linux / UNIX • Sieć Microsoft • Windows ACL • Zaawansowane uprawnienia do folderów (AFP, CIFS / SMB i FTP) • Agregacja folderów współdzielonych (CIFS / SMB) 24. PrintServer: • Maksymalna liczba drukarek: 3 • Obsługuje protokół drukowania internetowego • Wyświetlanie i zarządzanie zadaniami drukowania • Kontrola uprawnień na podstawie adresu IP i nazwy domeny 25. FTP Server: • FTP przez SSL / TLS (jawnie)			

		• Obsługa FXP 26. Manager plików: • Montaż napędu w chmurze dla Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive dla Firm, HiDrive, Amazon Cloud Drive, Yandex Disk and Box • Zdalne montowanie folderów współdzielonych (CIFS / SMB, FTP i WebDAV) • Przeglądanie dokumentów przy użyciu Office Online, Dokumentów Google i rozszerzenia Chrome • Edycja plików Microsoft Office przy użyciu Dokumentów, Arkuszy i Prezentacji Google 27. Backup i archiwizacja: • Automatyczne archiwizowanie • Funkcja przepisu • Archiwizacja przez iSCSI, USB, DVD i zdalny NAS • Kopia zapasowa w chmurze do Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Openstack Swift, WebDAV i HKBN • Synchronizacja magazynu w chmurze z Microsoft OneDrive, Dyskiem Google, Dropbox, Amazon Drive, Yandex Disk, Box, hubiC, BackBlaze B2, Amazon S3 i HiDrive • Serwer i klient RTRR z kontrolą przepustowości • Serwer Rsync z kontrolą przepustowości pobierania 28. Zarządzanie zdjęciami: • Organizacja zdjęć według miniatury, listy, osi czasu lub folderu • Albumy wirtualne i inteligentne • Kontrola ważności udostępniania albumów • Oznaczanie zdjęć tekstem, kolorami i ocenami • Pokazy slajdów z muzyką w tle i efektami przejścia • Geotagowanie zdjęć i wyświetlanie w Mapach Google			

		• Tworzenie kopii zapasowej i przywracanie konfiguracji albumu • Zaawansowane uprawnienia do folderów • Wsparcie dla użytkowników domeny • Photo manager: obsługuje wykrywanie twarzy i PDF do obrazu • Aplikacja mobilna do przeglądania i udostępniania online • wideo online 29. Wyszukiwanie: • Wyszukiwanie pełnotekstowe • Dystrybucja danych za pomocą wykresu słupkowego • Podgląd zdjęć, muzyki, filmów, plików PDF, Gmaila i innych • Zaawansowane operatory wyszukiwania i zakres wyszukiwania • Dostosowane filtry wyszukiwania z włączonymi lub wyłączonymi warunkami • Sugestia powiązanych plików w przeglądarce • Wyszukaj rozszerzenie Chrome 30. DLNA: • Obsługa telewizorów DLNA / UPnP i odtwarzaczy takich jak PlayStation 4 i Xbox One • Obsługa pliku indeksującego CUE dla APE i FLAC 31. Inne funkcje: • Lokalizacja NAS w tej samej sieci lokalnej • Montaż folderu współdzielonego NAS • Podstawowa konfiguracja ustawień (oprogramowanie układowe, serwer SMTP i ustawienia sieciowe) • Storage Plug & Connect (tylko Windows) • Przesyłanie multimediów (tylko Windows) 32. W komplecie: 2 x kable Ethernet, 2 x kable zasilające, komplet śrub do mocowania dysków HDD 3,5”, komplet śrub do mocowania dysków HDD 2,5”.			

2.	Dyski HDD przeznaczone do pracy z powyższym serwerem NAS	Dyski powinny spełniać poniżej wyspecyfikowane minimalne parametry: Dedykowane do pracy ciągłej w NAS. Obecne na liście kompatybilności producenta NAS. – wszystkie dyski jednakowe pod względem producenta, modelu, firmware oraz minimalnych danych technicznych przedstawionych poniżej: Pojemność – 10 TB Interfejs – SATA III (600) Pamięć podręczna – 256 MB Prędkość obrotowa – 7 200 obr/min. Średnia prędkość odczytu – 240 MB/s Średni czas między uszkodzeniami – 1000000 h Stopa błędów przy odczycie – 1:10E15	4	szt.	Minimum 60 miesięcy (gwarancja producenta)

Pakiet 4: Dostawa akcesoriów komputerowych:

Lp.	Przedmiot zamówienia	Opis - Parametry techniczne	Ilość zamawiana	Wielkość opakowania	Wymagany termin gwarancji
1.	Szafa z wyposażeniem dla serwerów i urządzeń teletechnicznych	Szafa powinna spełniać poniżej wyspecyfikowane parametry: Możliwość instalowania urządzeń teleinformatycznych i telekomunikacyjnych zgodnych ze standardem 19", Wymiary 42U, 800x1000 mm. Drzwi perforowane. Materiał – blacha stalowa. Otwory kablowe o szerokości 71 mm w płycie dolnej i górnej, pozwalające na wprowadzanie kabli zasilających z wtyczkami trójfazowymi. Wszystkie otwory w płycie dolnej i górnej zamknięte wyłamywanymi zaślepkami. Numeracja jednostek U na belkach nośnych. Minimalny kąt otwarcia drzwi przednich 170°. Możliwość zmiany kierunku otwierania drzwi. Możliwość ustawienia szafy bez stopek bezpośrednio na podłodze (brak wystających elementów pod szafą).	1	szt.	Minimum 12 miesięcy od daty dostawy

		Dopuszczalne obciążenie – nie mniej niż 800 kg dla szafy ustawionej na stopkach, cokole lub bezpośrednio na podłodze. Poniżej wyszczególniono wymagany osprzęt: • Panel wentylacyjny minimum 2 wentylatory. • Listwa zasilająca 19" gniazdo 9 x CEE 7/5 wtyk IEC320 C14, min. obciążenie 3500W, prąd znamionowy listwy min. 16A – 2 szt. • Półka min. 650mm gł. 4 pkt. Mocowania – 1 szt. W ramach dostawy Wykonawca dostarczy szafę do Zakładu Higieny Weterynaryjnej w Warszawie Oddział Terenowy w Ostrołęce ul. Składowa 8a i na miejscu zmontuje oraz ustawi we wskazanej przez Informatyka Zamawiającego lokalizacji. Osprzęt powinien być zamontowany do szafy w konfiguracji uzgodnionej z Informatykiem WIW w Siedlcach.			
2.	Czytnik kodów kreskowych	Laserowy ręczny czytnik kodów kreskowych USB z dodatkową podstawą w celu umożliwienia ustawienia go na biurku i możliwością automatycznego odczytu kodów po wykryciu zbliżonego dokumentu bez konieczności wciskania przycisku w czytniku	1	szt.	Minimum 12 miesięcy od daty dostawy
3.	Podkładka żelowa pod myszkę	Podkładka pod myszkę optyczną o parametrach: - pokryta od góry w całości jednorodną tkaniną w kolorze szarym lub grafitowym - zintegrowana żelowa poduszka pod nadgarstek - od spodu pod całością podkładki jednorodna gumowa lub gumo-podobna powłoka w kolorze czarnym zapobiegająca przemieszczaniu podkładki na biurku	23	szt.	Minimum 12 miesięcy od daty dostawy

Pakiet 5: Dostawa zasilaczy awaryjnych – UPS:

Lp.	Przedmiot zamówienia	Opis - Parametry techniczne	Ilość zamawiana	Wielkość opakowania	Wymagany termin gwarancji
1.	UPS - Zasilacz awaryjny	Zasilacz awaryjny powinien spełniać poniżej wyspecyfikowane minimalne parametry: • Interfejs: USB 2.0 (minimum jeden) • Moc pozorna: min. 3000 VA • Moc skuteczna: min. 2700 W • Liczba gniazd: min. 10 gniazd • Napięcie zasilania / zasilacza: 230 V • Topologia: online • Rodzaj wtyczki zasilającej: Typ E lub F • Certyfikaty: CE, CE Mark, EAC, EN/IEC 62040-1, EN/IEC 62040-2, RCM, VDE, REACH • Napięcie wejściowe: 230V • Maks. zniekształcenia harmoniczne THDi (mniej niż): 2 % • Obsługiwane zakresy częstotliwości: 50-60 Hz • Kształt przebiegu wyjściowego: sinusoida • Minimalna pojemność Akumulatora, VAh: 500 • Typ akumulatora: Bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu • Typ obudowy: tower (stojąca) • Panel sterowania Wielofunkcyjna konsola sterownicza i informacyjna z wyświetlaczem • Alarm: Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia.	3	szt.	Minimum 24 miesiące od daty dostawy

Pakiet nr 6: Dostawa urządzeń firewall:

Lp.	Przedmiot zamówienia	Opis - Parametry techniczne	Ilość zamawiana	Wielkość opakowania	Wymagany termin gwarancji
1.	Urządzenie zabezpieczenia brzegu sieci komputerowej - firewall	Dostawa urządzenia nowego i nie regenerowanego, o nie gorszych parametrach technicznych niż wskazano poniżej: **OBSŁUGA SIECI** 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP. **ZAPORA KORPORACYJNA (Firewall)** 2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 4. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 5. Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola	2	szt.	36 miesięcy u producenta urządzenia

		DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 7. Administrator powinien mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). **INTRUSION PREVENTION SYSTEM (IPS)** 10. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 11. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 12. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 13. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 14. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. 15. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 16. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i			

		docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. **KSZTAŁTOWANIE PASMA (Traffic Shapping)** 17. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 18. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 19. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 20. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. **OCHRONA ANTYWIRUSOWA** 21. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 22. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 23. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 24. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. **OCHRONA ANTYSPAM** 25. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 26. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL,			

		c. heurystyczny skaner. 27. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 28. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. **WIRTUALNE SIECI PRYWANTE (VPN)** 29. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 30. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 31. SSL VPN musi działać w trybach Tunel i Portal. 32. W ramach funkcji SSL VPN producent powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 33. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 34. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 35. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. **FILTR DOSTĘPU DO STRON WWW** 36. Urządzenie ma posiadać wbudowany filtr URL. 37. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 38. Administrator musi mieć możliwość dodawania własnych kategorii URL.			

		39. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 40. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 41. Administrator powinien posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 42. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 43. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 44. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 45. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 46. Urządzenie powinno posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 47. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. **UWIERZYTELNIANIE** 48. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 49. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 50. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:			

		a. SSL, b. Radius, c. Kerberos. 51. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 52. Co najmniej jedna z metod transparentnej autoryzacji nie powinna wymagać instalacji dedykowanego agenta. 53. Autoryzacja użytkowników z Microsoft Active Directory nie powinna wymagać modyfikacji schematu domeny. **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)** 54. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 55. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 56. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 57. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 58. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 59. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 60. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 61. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.			

		62. Rozwiązanie powinno wspierać technologię Link Aggregation. **POZOSTAŁE ROZWIĄZANIA USŁUGI I FUNKCJE** 63. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 64. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 65. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 66. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 67. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 68. Urządzenie musi posiadać usługę DNS Proxy. **ADMINISTRACJA URZĄDZENIEM** 69. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. 70. Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w języku polskim. 71. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową, a komunikacja musi być zabezpieczona za pomocą protokołu https. 72. Komunikacja powinna móc odbywać się na porcie innym niż https (443 TCP). 73. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 74. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.			

		75. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 76. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 77. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 78. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 79. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. **RAPORTOWANIE** 80. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 81. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 82. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 83. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów. 84. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 85. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.			

		86. Dodatkowy system powinien umożliwiać tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy **PARAMETRY SPRZĘTOWE** 87. Urządzenie ma być wyposażone w dysk o pojemności co najmniej 250 GB. 88. Liczba portów Ethernet 10/100/1000Mbps – min. 12. 89. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 90. Przepustowość Firewalla – min. 5 Gbps 91. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 3 Gbps. 92. Przepustowość filtrowania Antywirusowego – min. 850 Mbps 93. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1 Gbps. 94. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 500 95. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 100 96. Obsługa min. VLAN 256 97. Liczba równoczesnych sesji - min. 500 000 i nie mniej niż 20 000 nowych sesji/sekundę. 98. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 99. Urządzenie powinno być nielimitowane na użytkowników. 100. Każde z urządzeń musi mieć możliwość pracy jako drugie w klastrze HA dwóch urządzeń niniejszej specyfikacji, działających co najmniej w trybie Active/Passive 101. Wykonawca przy udziale pracownika Zamawiającego przeprowadzi wymianę dwóch urządzeń NETASQ U 150S			

		zainstalowanych w lokalizacji: siedziba główna Wojewódzkiego Inspektoratu Weterynarii z/s w Siedlcach, ul. Kazimierzowska 29, 08-110 Siedlce. Wykonawca przeniesie konfigurację jednego obecnego urządzenia na dostarczone urządzenie, drugie urządzenie skonfiguruje do pracy jako drugie w klastrze HA dwóch urządzeń niniejszej specyfikacji. Proces przenoszenia przez Wykonawcę konfiguracji i produkcyjne uruchomienie transmisji danych na dostarczanym urządzeniu nie może wpływać na utrzymanie ciągłości transmisji danych w trakcie godzin pracy. Wymieniane urządzenia pozostaną u Zamawiającego. 102. Do urządzeń powinny być załączone min. 3 miesięczne licencje dla następujących usług urządzenia: Firewall z mechanizmem Intrusion Prevention System, WIRTUALNE SIECI PRYWANTE (VPN), FILTR DOSTĘPU DO STRON WWW, OCHRONA ANTYWIRUSOWA, OCHRONA ANTYSPAM. Zakres funkcjonalny wymienionych usług urządzenia w okresie realizacji licencji czasowych powinien być zgodny i nie mniejszy niż określa niniejsza specyfikacja.			
2.	Urządzenie zabezpieczenia brzegu sieci komputerowej - firewall	Dostawa urządzenia nowego i nie regenerowanego, o nie gorszych parametrach technicznych niż wskazano poniżej: **OBSŁUGA SIECI** 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP. **ZAPORA KORPORACYJNA (Firewall)** 2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.	2	szt.	36 miesięcy u producenta urządzenia

		4. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 5. Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 7. Administrator powinien mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). **INTRUSION PREVENTION SYSTEM (IPS)** 10. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.			

		11. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 12. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 13. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 14. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. 15. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 16. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. **KSZTAŁTOWANIE PASMA (Traffic Shapping)** 17. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 18. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 19. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 20. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. **OCHRONA ANTYWIRUSOWA** 21. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).			

		22. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 23. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 24. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. **OCHRONA ANTYSPAM** 25. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 26. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner. 27. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 28. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. **WIRTUALNE SIECI PRYWANTE (VPN)** 29. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 30. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 31. SSL VPN musi działać w trybach Tunel i Portal.			

		32. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 33. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 34. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 35. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. **FILTR DOSTĘPU DO STRON WWW** 36. Urządzenie ma posiadać wbudowany filtr URL. 37. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 38. Administrator musi mieć możliwość dodawania własnych kategorii URL. 39. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 40. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 41. Administrator powinien posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 42. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 43. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 44. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.			

		45. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 46. Urządzenie powinno posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 47. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. **UWIERZYTELNIANIE** 48. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 49. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 50. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 51. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 52. Co najmniej jedna z metod transparentnej autoryzacji nie powinna wymagać instalacji dedykowanego agenta. 53. Autoryzacja użytkowników z Microsoft Active Directory nie powinna wymagać modyfikacji schematu domeny. **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)** 54. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 55. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia.			

		56. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 57. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 58. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 59. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 60. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 61. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. **POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA** 62. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 63. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 64. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 65. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 66. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 67. Urządzenie musi posiadać usługę DNS Proxy. **ADMINISTRACJA URZĄDZENIEM** 68. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.			

		69. Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w języku polskim. 70. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 71. Komunikacja powinna móc odbywać się na porcie innym niż https (443 TCP). 72. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 73. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 74. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 75. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 76. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 77. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 78. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. **RAPORTOWANIE** 79. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.			

		80. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 81. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 82. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. 83. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 84. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 85. Dodatkowy system powinien umożliwiać tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy **PARAMETRY SPRZĘTOWE** 86. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 87. Liczba portów Ethernet 10/100/1000Mbps – min. 8. 88. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 89. Przepustowość Firewalla – min. 3,5 Gbps 90. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 2,4 Gbps. 91. Przepustowość filtrowania Antywirusowego – min. 400 Mbps 92. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 600 Mbps. 93. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100.			

		94. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. 95. Obsługa min. VLAN 64 96. Liczba równoczesnych sesji - min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę. 97. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 98. Urządzenie powinno być nielimitowane na użytkowników. 99. Urządzenie musi być wyposażone dodatkowo w nośnik pamięci flash o pojemności minimum 64 GB (gwarancja na pamięć min. 12 miesięcy) 100. Wykonawca dostarczy dedykowane rozwiązanie do tworzenia raportów w formie maszyny wirtualnej do zainstalowania w środowisku zamawiającego dla wszystkich urządzeń niniejszej specyfikacji. 101. Wykonawca przy wsparciu pracownika Zamawiającego wymieni urządzenia NETASQ U 70S zainstalowanego w lokalizacji: Zakład Higieny Weterynaryjnej w Warszawie, ul. Lechicka 21, 02-156 Warszawa oraz urządzenia NETASQ U 30S zainstalowanego w lokalizacji: Zakład Higieny Weterynaryjnej w Warszawie Oddział Terenowy w Ostrołęce, ul. Składowa 8A, 07-411 Ostrołęka. Wykonawca przeniesie konfigurację obecnych urządzeń na dostarczone urządzenia. Proces przenoszenia przez Wykonawcę konfiguracji i produkcyjne uruchomienie transmisji danych na dostarczanym urządzeniu nie może wpływać na utrzymanie ciągłości transmisji danych w trakcie godzin pracy. Wymieniane urządzenia pozostaną u Zamawiającego. 102. Do urządzenia powinny być załączone min. 3-miesięczne licencje dla następujących usług urządzenia: Firewall z mechanizmem Intrusion Prevention System, WIRTUALNE SIECI PRYWANTE (VPN), FILTR DOSTĘPU			

		DO STRON WWW, OCHRONA ANTYWIRUSOWA, OCHRONA ANTYSPAM. Zakres funkcjonalny wymienionych usług urządzenia w okresie realizacji licencji czasowych powinien być zgodny i nie mniejszy niż określa niniejsza specyfikacja. Wykonawca przeprowadzi jednodniowe warsztaty techniczne ze wszystkich urządzeń niniejszego pakietu w języku polskim dla dwóch pracowników Zamawiającego w siedzibie i na urządzeniach Wykonawcy w terminie do 31 marca 2020 roku.			

ROZDZIAŁ XVII SIWZ – INFORMACJE DODATKOWE.

I. Informacja o sposobie przetwarzania danych osobowych w Wojewódzkim Inspektoracie Weterynarii z siedzibą w Siedlcach w związku z realizacją zamówień publicznych.

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

1. Administratorem Pani/Pana danych osobowych jest Mazowiecki Wojewódzki Lekarz Weterynarii.
2. Kontakt z inspektorem ochrony danych osobowych jest możliwy w formie elektronicznej na skrzynkę iod@wiw.mazowsze.pl.
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego: **Dostawa oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach** - nr sprawy: **WIW-AD.272.97.2019**

   /dane identyfikujące postępowanie, np. nazwa, numer/

   prowadzonym w trybie przetargu nieograniczonego;
4. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2018 r. poz. 1986, z późniejszymi zmianami), dalej „ustawa Pzp" oraz Wojewoda Podlaski w związku z korzystaniem przez *Wojewódzki Inspektorat Weterynarii z systemu elektronicznego zarządzania dokumentacją (EZD PUW)*;
5. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 5 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 5 lata, okres przechowywania obejmuje cały czas trwania umowy;
6. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
7. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
8. Posiada Pani/Pan:
   – na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;

- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;
- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

9. Nie przysługuje Pani/Panu: − w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych; − prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO; − na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

Załącznik nr 1 do SIWZ

Nr sprawy: WIW-AD.272.97.2019

OŚWIADCZENIE O NIEPODLEGANIU WYKLUCZENIU ORAZ SPEŁNIENIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Nazwa i adres Wykonawcy: .....
.....
.....

Przystępując do postępowania o udzielenie zamówienia publicznego na **dostawę oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach** oświadczam, że:

1. nie podlegam wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 24 ust. 1 pkt od 12 do 23 ustawy Prawo zamówień publicznych,
2. spełniam warunki udziału w postępowaniu o udzielenie zamówienia publicznego określone przez zamawiającego w niniejszym postępowaniu.
3. Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ..... ustawy Pzp (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 24 ust. 1 pkt 13-14, 16-20 ustawy Pzp). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze:

   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
4. Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w Rozdziale II Specyfikacji

Istotnych Warunków Zamówienia oraz Ogłoszeniu o zamówieniu, polegam na zasobach następującego/ych podmiotu/ów:

……

……

w następującym zakresie:

……

……

(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).

5. Oświadczam, że w stosunku do następującego/ych podmiotu/tów, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.: …… (podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG) nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.
6. Oświadczam, że następujący/e podmiot/y, będący/e podwykonawcą/ami: …… *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*, nie podlega/ą wykluczeniu z postępowania o udzielenie zamówienia.
7. Wszystkie informacje podane w niniejszym oświadczeniu są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawieniu informacji.

_____ dnia __ __ 2019 rok

_____

(podpis osób wskazanych w dokumencie uprawniającym do wystąpienia w obrocie prawnym lub posiadającym pełnomocnictwo)

Załącznik nr 2 do SIWZ

Nr sprawy: WIW-AD.272.97.2019

OŚWIADCZENIE WYKONAWCY DOTYCZĄCE GRUPY KAPITAŁOWEJ

My niżej podpisani, działając w imieniu i na rzecz:
.....
.....
(pełna nazwa (firma) dokładny adres Wykonawcy)
W przypadku składania oferty przez Wykonawców występujących wspólnie oświadczenie składa każdy z wykonawców.

ubiegając się o udzielenie zamówienia publicznego na **dostawę oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach**,

oświadczam, **że należę* / reprezentowany przeze mnie podmiot należy do grupy kapitałowej*,** w rozumieniu przepisów ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r., poz. 369) do której należą także następujące podmioty*:

1.....;

2.....;

3.....;

oświadczam, że: **nie należę* / reprezentowany przeze mnie podmiot nie należy do grupy kapitałowej***, o której mowa w art. 24 ust. 1 pkt 23 ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (Dz. U. z 2018 r., poz. 1986 z późn. zm.)*.

_____ dnia __ __ 2019 rok

_____

(podpis osób wskazanych w dokumencie uprawniającym do wystąpienia w obrocie prawnym lub posiadającym pełnomocnictwo)

** niepotrzebne skreślić*

Załącznik nr 3 do SIWZ

Nr sprawy: WIW-AD.272.97.2019

OFERTA

Do:

Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach

ul. Kazimierzowska 29, 08-110 Siedlce.

(nazwa i adres Zamawiającego)

Nawiązując do ogłoszenia w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na **dostawę oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach,**

– Pakiet nr ...

my niżej podpisani:

……

……

działając w imieniu i na rzecz:

……

……

(nazwa (firma) dokładny adres Wykonawcy/ Wykonawców); w przypadku składania oferty przez podmioty występujące wspólnie podać nazwy (firmy) i dokładne adresy wszystkich podmiotów składających wspólną ofertę)

1. **OŚWIADCZAMY**, że naszym pełnomocnikiem dla potrzeb niniejszego zamówienia jest:

……

(Wypełniają jedynie przedsiębiorcy składający wspólną ofertę)

2. **SKŁADAMY OFERTĘ** na wykonanie przedmiotu zamówienia zgodnie ze Specyfikacją Istotnych Warunków Zamówienia za cenę w wysokości:

Lp.	Przedmiot zamówienia**	Producent	Numer katalogowy/ model **	Termin gwarancji	J.m.	Cena jedn. netto dostawy (bez VAT) w zł	Ilość J.m.	Wartość dostawy netto (bez VAT) w zł	Stawka VAT %	Kwota VAT w zł	Wartość dostawy brutto w zł *
1	2	3	4	5	6	7	8	9	10	11	12
CENA OFERTY (DOSTAWY) NETTO (należy dodać do siebie poszczególne pozycje z kolumny 10)									—	—	—
RAZEM KWOTA VAT (należy dodać do siebie poszczególne pozycje z kolumny 12)											—
CENA OFERTY (DOSTAWY) BRUTTO (należy dodać do siebie poszczególne pozycje z kolumny 13)											
Słownie brutto:											

* Gdy Wykonawca nie jest zobowiązany do naliczenia VAT należy wpisać kwotę z pozycji 9 (wartość dostawy netto bez VAT).
** Zamawiający wymaga wyceny każdego rodzaju oferowanego sprzętu oddzielenie.

3. Informuję/jemy, że złożona oferta zamówienia **prowadzi*/ nie prowadzi*** do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług oraz ustawą (Dz.U. z 2011r. poz. 1054 z późn. zmianami) – Prawo zamówień publicznych (art. 91 ust. 3a ustawy Pzp). Obowiązek podatkowy u Zamawiającego (tzw. „mechanizm odwróconego VAT", *podatek VAT rozliczany jest przez Zamawiającego, a nie Wykonawcę*) dotyczy następujących dostaw towarów..... ..... o wartości wynoszącej bez podatku ..... złotych
4. **OŚWIADCZAMY,** że jesteśmy/nie jesteśmy* podatnikiem VAT o numerze ..... zarejestrowanym w ..... (podać kraj) i przez cały czas trwania umowy będziemy się posługiwać podanym wyżej numerem.

Podmiotem uprawnionym do wystawienia faktur przez cały czas trwania umowy jest .....

.....

(*w przypadku wykonawców wspólnie składający ofertę).*

5. **OŚWIADCZAMY,** że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia i uznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania.
6. **ZOBOWIĄZUJEMY SIĘ** do wykonania zamówienia w terminie określonym w Specyfikacji Istotnych Warunków Zamówienia.
7. **OŚWIADCZAMY,** iż termin płatności wynosi …… **dni od dnia otrzymania przez Zamawiającego faktury VAT**.
8. **UWAŻAMY SIĘ** za związanych niniejszą ofertą przez czas wskazany w Specyfikacji Istotnych Warunków Zamówienia, tj. przez okres **30 dni** od upływu terminu składania ofert.
9. **OŚWIADCZAMY,** że zapoznaliśmy się z wzorem umowy i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach określonych w Specyfikacji Istotnych Warunków Zamówienia, w miejscu i terminie wyznaczonym przez Zamawiającego.
10. **OŚWIADCZAMY,** że informacje stanowiące tzw. tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji, zostały umieszczone w odrębnej kopercie z adnotacją „Tajemnica przedsiębiorstwa” TAK / NIE*
11. **OŚWIADCZAMY**, iż zaliczamy się do małych i średnich przedsiębiorstw **TAK/NIE*.**
12. **ZAMÓWIENIE ZREALIZUJEMY** sami/przy udziale podwykonawców*, którzy będą wykonywać następujące prace wchodzące w zakres przedmiotu zamówienia:

a) ……

(opis zamówienia zlecanego podwykonawcy)

b) ……

(opis zamówienia zlecanego podwykonawcy)

13. **WSZELKĄ KORESPONDENCJĘ** w sprawie niniejszego postępowania należy kierować na adres:
    tel. .....
    adres poczty elektronicznej .....
    osoba wyznaczona do kontaktu z Zamawiającym .....
14. **OFERTĘ** niniejszą składamy na ..... kolejno ponumerowanych stronach.
15. **PRZEDKŁADAMY** do oferty następujące oświadczenia i dokumenty:

    a/ .....str. oferty .....
    b/ ..... str. oferty .....
    c/ ..... str. oferty .....
    d/ ..... str. oferty .....

_____ dnia __ __ 2019 rok

_____

(podpis osób wskazanych w dokumencie uprawniającym do wystąpienia w obrocie prawnym lub posiadającym pełnomocnictwo)

*** - niepotrzebne skreślić**

Załącznik nr 4 do SIWZ

Nr sprawy: WIW-AD.272.97.2019

U M O W A nr WIW-AD.273. ... .2019

zawarta w dniu ..... 2019 roku pomiędzy:
Skarbem Państwa - Wojewódzkim Inspektoratem Weterynarii z siedzibą w Siedlcach;
ul. Kazimierzowska 29;
08-110 Siedlce;
reprezentowanym przez:
.....
.....
zwanym dalej w treści umowy **„Zamawiającym”**
a firmą
.....
.....
reprezentowanym przez:
.....
.....
zwanym dalej w treści umowy **„Wykonawcą”,** w wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego poniżej równowartości 144.000 EURO, **Nr sprawy: WIW-AD.272.97.2019 – Pakiet nr .....,** zgodnie z ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2018 r., poz. 1986 z późn. zm.), została zawarta umowa o następującej treści.

§ 1

1. Przedmiotem niniejszej umowy jest **dostawa oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach – Pakiet 1 .....**, zgodnie z zestawieniem asortymentowo - cenowym stanowiącym **Załącznik nr 1** niniejszej umowy.
2. Wykonawca zobowiązuje się w ramach realizacji przedmiotu tej umowy, do dostarczenia przedmiotu zamówienia, własnym transportem i na swój koszt.

§ 2

1. Przedmiot niniejszej umowy wskazany w § 1, dostarczany będzie przez Wykonawcę zgodnie z harmonogramem dostaw stanowiącym **Załącznik nr 2** do niniejszej umowy.
2. W dniu dostarczenia przedmiotu zamówienia Wykonawca wystawi fakturę VAT, która po potwierdzeniu dostarczenia przedmiotu umowy stanowić będzie podstawę rozliczeń między stronami.
3. Fakturę VAT za dostarczony przedmiot zamówienia Wykonawca prześle bezpośrednio do Zamawiającego, tj. Wojewódzki Inspektorat Weterynarii z siedzibą w Siedlcach ul. Kazimierzowska 29, 08-110 Siedlce.

§ 3

1. Potwierdzeniem dostarczenia przedmiotu zamówienia będzie Protokół Odbioru sporządzony przez Wykonawcę wg wzoru stanowiącego **Załącznik nr 3** niniejszej umowy.
2. Protokół Odbioru sporządzony będzie w 3 jednobrzmiących egzemplarzach (jeden egzemplarz dla Wykonawcy, i dwa egzemplarze dla Zamawiającego) oryginalnie podpisanych i ostemplowanych przez upoważnione osoby:
   a) Ze strony Zamawiającego:
      – .....
      – .....
      lub inne upoważnione osoby.
   b) Ze strony Wykonawcy:
      – .....
      lub inne upoważnione osoby.
3. Podpisanie Protokołu Odbioru nastąpi w dniu dostarczenia przedmiotu zamówienia.

§ 4

1. Wykonawca udziela Zamawiającemu gwarancji na dostarczony przedmiot zamówienia zgodnie z treścią **Załącznika nr 1** do niniejszej umowy.
2. Zamawiający ma obowiązek zawiadomienia Wykonawcy o zaistniałej wadzie przedmiotu umowy w ciągu 7 dni od dnia jej stwierdzenia.
3. Wykonawca zobowiązuje się do uwzględnienia reklamacji wad przedmiotu umowy w terminie 14 dni od dnia pisemnego zgłoszenia reklamacji przez Zamawiającego.

§ 5

W przypadku opóźnienia w wykonaniu umowy w zakresie terminu realizacji, Zamawiający może od Wykonawcy:

a) żądać zapłacenia kary umownej w wysokości 0,5 % kwoty wynagrodzenia za niedostarczenie w terminie partii towaru, za każdy dzień opóźnienia, nie wyższej jednak niż 10 % wartości przedmiotu zamówienia. Zapłata kary umownej nastąpi w terminie 14 dni od wezwania skierowanego przez Zamawiającego do Wykonawcy listem poleconym. Wezwanie do zapłaty kary umownej zawierało będzie każdorazowo szczegółowe wyliczenie wysokości naliczonej kary umownej,
b) wyznaczyć dodatkowy termin do wykonania umowy, przy zachowaniu prawa do naliczania kary umownej w wysokości określonej w punkcie a) za każdy dzień opóźnienia,
c) rozwiązać umowę bez wypowiedzenia przy przekroczeniu terminu wyznaczonego w trybie pkt b), przy zachowaniu prawa do naliczania kary umownej w wysokości określonej w punkcie a).

§ 6

1. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie będzie leżeć w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, zamawiający będzie mógł odstąpić od

umowy w terminie miesiąca od powzięcia wiadomości o powyższych okolicznościach.
2. W przypadku rozwiązania umowy przez Zamawiającego Wykonawca otrzyma wynagrodzenie stosowne do zakresu wykonanego zamówienia. Zakres wykonanego zamówienia zostanie określony przez Strony po dokonaniu wypowiedzenia umowy.
3. W przypadku rozwiązania umowy przez Wykonawcę lub z przyczyn leżących po stronie Wykonawcy, Zamawiający zastrzega sobie prawo żądania otrzymania kary umownej w wysokości 10 % wartości niezrealizowanego przedmiotu zamówienia. Zapłata kary umownej nastąpi w terminie 14 dni od wezwania skierowanego przez Zamawiające do Wykonawcy listem poleconym. Wezwanie do zapłaty kary umownej zawierało będzie szczegółowe wyliczenie wysokości naliczonej kary umownej.
4. Zamawiający, w razie wykazania szkody przewyższającej karę umowną, może dochodzić od Wykonawcy odszkodowania uzupełniającego na zasadach ogólnych.

§ 7

1. Strony ustalają, całkowite wynagrodzenie za realizację przedmiotu zamówienia w wysokości ..... **zł brutto** (**słownie:** ....).
2. Wynagrodzenie określone w ust. 1 obejmuje także koszty, jakie zostaną poniesione przez Wykonawcę dla wykonania zadań objętych niniejszą umową.
3. Maksymalne wynagrodzenie brutto podane w ust. 1 może ulec zmianie tylko w sytuacji określonych w § 10 pkt. 2 umowy oraz w przypadku zastosowania prawa opcji przez Zamawiającego.

§ 8

1. Rozliczenie dostaw nastąpi na podstawie faktur VAT dostarczonych do siedziby Zamawiającego.
2. Faktury uregulowane zostaną w terminie **..... dni** od dnia ich otrzymania przez Zamawiającego.
3. W przypadku opóźnienia w płatnościach, o których mowa powyżej przez Zamawiającego na rzecz Wykonawcy, Wykonawcy przysługuje prawo naliczania odsetek ustawowych za każdy dzień opóźnienia.

§ 9

1. W przypadku powstania sporów związanych z realizacją postanowień niniejszej umowy w sprawie zamówienia publicznego, Zamawiający zobowiązany jest wyczerpać drogę postępowania reklamacyjnego, kierując swoje roszczenie do Wykonawcy.
2. W razie niezadowalającego rozstrzygnięcia reklamacyjnego, Zamawiającemu przysługuje prawo wystąpienia do sądu powszechnego. Sądem miejscowo właściwym będzie odpowiedni Sąd właściwy dla siedziby Zamawiającego.
3. W sprawach nieuregulowanych niniejszą umową zastosowanie znajdują postanowienia ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (Dz. U. z 2018 r., poz. 1986, z późn. zm.) oraz przepisy Kodeksu Cywilnego.

§ 10

1. Wszelkie zmiany niniejszej umowy wymagają dla swojej ważności formy pisemnej pod rygorem nieważności.
2. Dopuszcza się możliwość zmiany umowy w zakresie zmiany obowiązującej stawki podatku VAT w przypadku ustawowej zmiany stawki podatku VAT.

§ 11

Umowę sporządzono w trzech jednobrzmiących egzemplarzach: 1 egzemplarz dla Wykonawcy i 2 egzemplarze dla Zamawiającego.

ZAMAWIAJĄCY WYKONAWCA

Załącznik nr 1
do umowy nr WIW-AD.273. … .2019

ZESTAWIENIE ASORTYMENTOWO – CENOWE

Lp.	Przedmiot Zamówienia (nazwa, producent, numer katalogowy)	Termin gwarancji	J.m.	Wielkość J.m.	Cena jedn. netto dostawy (bez VAT) w zł	Ilość J.m.	Wartość dostawy netto (bez VAT) w zł	Stawka VAT %	Kwota VAT w zł	Wartość dostawy brutto w zł
RAZEM:										

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 2
do umowy nr WIW-AD.273. ... .2019

HARMONOGRAM DOSTAW

Miejsce realizacji dostaw: .....

Lp.	Przedmiot zamówienia	Ilość zamawiana	Termin dostawy

ZAMAWIAJĄCY WYKONAWCA

Załącznik nr 3
do umowy nr WIW-AD.273. ... .2019

PROTOKÓŁ ODBIORU

PRZEPROWADZONEGO W:

.....

.....

.....

Dzień odbioru: .....

I. Biorący udział:

Ze strony Wykonawcy - (*nazwa i adres sprzedającego*)

.....

p.....

(*nazwisko i imię*)

p.....

(*nazwisko i imię*)

Ze strony Zamawiającego - (*nazwa i adres odbierającego*)

.....

p.....

(*nazwisko i imię*)

II. Przedmiot dostawy i odbioru w ramach Umowy nr .....
z dnia .....

Lp.	Przedmiot Zamówienia (nazwa, producent, numer katalogowy)	Ilość	Wartość w zł netto (zgodnie z umową)	Wartość w zł brutto (zgodnie z umową)

III. Kompletność dostawy[1]:
   1. TAK
   2. NIE - uwagi / zastrzeżenia:

   .....

   .....

IV. Kontrola ilościowa i jakościowa[1]:
   1. Pozytywny
   2. Negatywny - uwagi / zastrzeżenia:

   .....

   .....

V. Gwarancja .....

VI. Końcowy wynik przyjęcia[1]:
   1. Pozytywny
   2. Negatywny - uwagi / zastrzeżenia:

   .....

   .....

Podpisy:

.....	.....
Ze strony Zamawiającego	*Ze strony Wykonawcy*
imię, nazwisko, pieczątka	*imię, nazwisko, pieczątka*

[1] Niepotrzebne skreślić

Załącznik nr 5 do SIWZ

Nr sprawy: WIW-AD.272.97.2019

SPECYFIKACJA OFEROWANEGO PRZEDMIOTU ZAMÓWIENIA

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na **dostawę oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach,**

Pakiet 1: Dostawa urządzeń wielofunkcyjnych:

___	**Parametry Zamawiającego**		**Oferowane przez Wykonawcę parametry***	
Lp.	**Przedmiot zamówienia**	**Opis - Parametry techniczne**	**Przedmiot zamówienia (nazwa, producent, numer katalogowy***	**Parametry techniczne***
1.	Urządzenie wielofunkcyjne (drukarka/ kopiarka/ skaner)	Urządzenia powinny spełniać poniżej wyspecyfikowane minimalne parametry: 1. Minimalna prędkość wydruku A4/min - 40ppm (BW/kolor); 2. Minimalna prędkość wydruku A3/min 22ppm; 3. Format oryginału - minimum A3; 4. Pamięć RAM minimum - 4 GB; 5. Maksymalny czas uzyskania 1. kopii - BW 4,5 sek., kolor 6.5 sek.; 6. Czas uruchomienia do 22sek.; 7. Minimalna pojemność papieru - 1200 arkuszy; 8. Minimalna pojemność podajnika bocznego - 100 arkuszy;		

		9. Minimalna ilość źródeł papieru – 3; 10. Wydruk na kopertach z automatycznym podawaniem; 11. Minimalny zakres gramatur papieru od 52 do 300g/m2; 12. Automatyczny druk / kopia dwustronna; 13. Interfejsy: Ethernet (1000BaseT/100Base-TX/10Base-T), USB, bezprzewodowa sieć LAN (IEEE 802.11 b/g/n); 14. Język drukarki: PCL 6, PostScript Level 3; 15. Minimalna pojemność dysku drukarki - 250 GB; 16. Minimalna rozdzielczość kopiowania - 600dpi×600dpi; 17. Minimalna rozdzielczość drukowania - 600dpi×600dpi; 18. Automatyczny dwustronny, jednoprzebiegowy podajnik oryginałów.; 19. Minimalna pojemność podajnika oryginałów: 150 arkuszy; 20. Minimalna prędkość skanowania - 80 stron A4/min jednostronnie; 160 stron A4/min dwustronnie; 21. Skanowanie z wysyłaniem na adresy email, zasoby SMB, zasoby FTP, pamięci USB; 22. Format zapisywanych plików - TIFF, JPEG, PDF, Przeszukiwany PDF, Szyfrowany PDF, XPS, Office Open XML (PowerPoint, Word), PDF/XPX , PDF/A-1b , Sygnatura cyfrowa; 23. Szafka pod urządzenie umożliwiająca postawienie go na podłodze;		

		24. Czytnik kart zbliżeniowych; 25. System zarzadzania uwierzytelnianiem: W okresie co najmniej 5 lat od dostarczenia urządzeń wykonawca powinien zapewnić działanie jednolitego systemu umożliwiającego logowanie się na urządzeniach za pomocą kart zbliżeniowych. System powinien obsługiwać urządzenia dotychczas znajdujące się w użytkowaniu przez zamawiającego (CANON iRAC 5235i – ilość: 6szt., iRAC 5030i – ilość: 10szt.) 26. Uwierzytelnienie - kontrola funkcji urządzenia (kopiowanie, drukowania, wysyłanie, kolor, druk jednostronny), automatyczne zwalnianie wydruków po zalogowaniu, podgląd wydruku przed zwolnieniem, funkcja wymuszonego wstrzymania wydruku, funkcja wyślij do mnie; 27. Wspólna dla wszystkich maszyn baza użytkowników, nie powinna wymagać zasobów sprzętowych po stronie zamawiającego, jeżeli jest taka konieczność wykonawca dostarczy stosowne zasoby komputerowe. Integracja z AD. 28. Raporty użycia z podziałem na urządzenie, użytkownika, grupę, z możliwością zebrania danych z wielu urządzeń. Raport musi zawierać cenę wykonanych prac. 29. System monitorowania urządzeń: Wykonawca powinien zapewnić rozwiązanie pozwalające w okresie co najmniej 5 lat od daty uruchomiania monitorowanie stanu urządzeń z powiadamianiem o :		

		• Małej ilości tonera, błędach, zacięciach papieru, stanie liczników, stopniu zużycia części. • System powinien obsługiwać urządzenia dotychczas znajdujące się w użytkowaniu przez zamawiającego. (CANON iRAC 5235i, iRAC 5030i) 30. Zabezpieczenie dokumentu: • Bezpieczne drukowanie, szyfrowane pliki PDF, podpis urządzenia, zabezpieczające znaki wodne. • Zabezpieczenie danych moduł TPM (Trusted Platform Module), wymazywanie dysku twardego (DoD, minimum 9 razy losowymi danymi), szyfrowanie dysku twardego (FIPS140-2, zatwierdzone); 31. Wydajność czarnego tonera/ów dostarczonego z urządzeniem - min. 60 000 wydruków przy pokryciu 5%; 32. Wydajność kolorowych tonerów dostarczonych z urządzeniem - min. 22 000 wydruków przy pokryciu 5% ; 33. Wydajność bębnów - Min. 125 000 wydruków • Tonery dostarczone z urządzeniem powinny być kompletnym zestawem tonerów tego samego producenta co urządzenie 34. Oferta powinna uwzględniać dostarczenie, instalację urządzeń wraz z konfiguracją (podłączenie do Active Directory) i wygenerowaniem pierwszych wydruków		

		testowych oraz przesłanie skanów na lokalizację sieciową.		

*do wypełnienia przez Wykonawcę, zapisy „Tak", „Zgodnie", czy „Spełnia" „Jak obok" nie będą akceptowane, należy podać precyzyjnie rzeczywisty oferowany parametr. Wypełniają Wykonawcy składający ofertę na dany pakiet.

_____ dnia __ __ 2019 rok

_____

(pieczęć i podpis)

Pakiet 2: Dostawa oprogramowania do kompleksowego zarządzania zasobami IT:

__	**Parametry Zamawiającego**		**Oferowane przez Wykonawcę parametry***	
Lp	**Przedmiot zamówienia**	**Opis - Parametry techniczne**	**Przedmiot zamówienia (nazwa, producent, numer katalogowy***	**Parametry techniczne***
1.	Oprogramowanie do kompleksowego zarządzania zasobami IT	**Oprogramowanie powinno spełniać niżej wyspecyfikowane minimalne parametry:** 1. Oprogramowanie powinno posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Moduły powinny umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. 2. Powinno monitorować infrastrukturę (bezagentowo) obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie (moduł sieciowy): • Serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych		

		serwisów. Mieć możliwość monitorowania czas ich odpowiedzi i procent utraconych pakietów. • Serwerów pocztowych: – monitorować zarówno serwis odbierający, jak i wysyłający pocztę, – możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem), – możliwość wykonywania operacji testowych, – możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa. • Monitorowania serwerów WWW i adresów URL. • Obsługi szyfrowania SSL/TLS w powiadomieniach e-mail. • Obsługi urządzeń SNMP wspierających SNMP v1/2/3 (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.). • Obsługi komunikatów syslog i pułapek SNMP. • Monitoringu routerów i przełączników wg: – zmian stanu interfejsów sieciowych, – ruchu sieciowego, – podłączonych stacji roboczych, – ruchu generowanego przez podłączone stacje robocze. • Serwisów Windows: monitor serwisów Windows alarmuje, gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie. • Wydajności systemów Windows: – obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. Program powinien posiadać Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz		

		tworzyć dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). 3. W zakresie inwentaryzacji program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz: a) Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. b) Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. c) Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows, co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. d) Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. e) Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. f) Umożliwiać odczytanie numeru seryjnego (klucze licencyjne). Moduł inwentaryzacji sprzętu powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie: • przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, • definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości – dla danego urządzenia lub oprogramowania powinna		

		istnieć możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX), skan dowolnego dokumentu, czy też własny komentarz; dodatkowo powinna być możliwość importu danych z zewnętrznego źródła (.CSV), • generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania, • archiwizacji i porównywania audytów środków trwałych, • tworzenia kodów kreskowych w Środkach Trwałych, • drukowania kodów kreskowych oraz QR Code (mozaikowe) dla środków trwałych, które posiadają numer inwentarzowy, inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej na system Android. Powinny być dostępne Agenty inwentaryzacji na systemy Android, OS X oraz Linux. Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: a) Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. b) Zarządzanie posiadanymi licencjami. c) Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili powinna		

		istnieć możliwość wykonania aktualnych raportów audytowych. d) Zarządzanie posiadanymi licencjami: raport zgodności licencji. e) Możliwość przypisania do programów numerów seryjnych, wartości itp. Okna audytowe powinny posiadać możliwość filtrowania elementów per oddział. 4. W zakresie obsługi użytkowników program Powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez analizę: • Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), • Monitorowanie procesów (każdy proces - całkowity czas działania oraz czas aktywności użytkownika), • Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona), • Informacji o edytowanych przez użytkownika dokumentach, • Historii pracy (cykliczne zrzuty ekranowe), • Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt), • Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), • Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek		

		poprzez identyfikację drukarek. Możliwość monitorowania kosztów wydruków, • Nagłówków przesyłanej poczty e-mail. Program ponadto powinien posiadać możliwość blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.onet.pl). Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji. 5. Program Powinien umożliwiać realizację zdalnej pomocy użytkownikom. W ramach kontroli stacji użytkownika powinien być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu powinien mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module powinna znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, wpisywane i widoczne dla obu stron. Moduł ten powinien zawierać również komunikator (czat), który umożliwi przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najbardziej typowe problemy.		

		Moduł pomocy zdalnej powinien umożliwić również: • pobieranie listy użytkowników z Active Directory, • przypisywanie pracowników helpdesk do kategorii zgłoszeń, • procesowanie zgłoszeń użytkowników z wiadomości e-mail, • dołączanie załączników do zgłoszeń, • zrzuty ekranowe (podgląd pulpitu), • dystrybucję oprogramowania przez Agenty, • dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), • zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, • możliwość skonfigurowania automatyzacji procesowania zgłoszeń, • planowanie nieobecności pracowników helpdesk, • generowanie raportów obsługi helpdesk 6. Możliwość ochrony danych przed wyciekiem poprzez blokowanie urządzeń. a) Blokowanie urządzeń i nośników danych. b) Możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. c) Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. d) Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. e) Blokownie powinno dotyczyć urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) powinny móc pozostać. Zarządzanie prawami dostępu do urządzeń:		

		a) Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. b) Autoryzowanie urządzeń wskazanych: pendrive'ów, dysków itp. c) Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników lub stacji roboczych. d) Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci lub wybranych stacji roboczych. Audyt operacji na urządzeniach przenośnych: a) Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. b) Podłączenie/odłączenie urządzenia przenośnego. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. 7. Ochrona przed usunięciem oprogramowania. Program powinien mieć możliwość zabezpieczenia hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet, jeśli użytkownik ma prawa administratora. 8. Program powinien być dostępny w języku polskim. 9. Oferowane oprogramowanie powinno umożliwić w pełni funkcjonalne zarządzanie i monitorowanie minimum 200 urządzeń sieciowych. 10. W ramach dostawy oprogramowania, Wykonawca zobowiązuje się do przeprowadzenia zaawansowanego nieodpłatnego szkolenia technicznego w języku polskim , zapewniającego zdobycie wiedzy niezbędnej do projektowania, wdrażania i optymalizowania rozwiązań wykorzystujących przedmiotowe oprogramowanie a także umiejętność rozwiązywania ewentualnych problemów. Szkolenie powinno odbyć się w centrum treningowym, certyfikowanym przez producenta oprogramowania.		

		Realizacja szkolenia powinna być przeprowadzona według następujących założeń: • Szkolenie powinno być przeprowadzone dla dwóch administratorów systemu Zamawiającego. • Każdy uczestnik szkolenia powinien otrzymać odpowiednie świadectwo (certyfikat) o jego odbyciu. • Szkolenie powinno zostać przeprowadzone przez osoby posiadające odpowiednie kwalifikacje, potwierdzone certyfikatem producenta oprogramowania. • W ramach szkolenia Wykonawca powinien zapewnić szkolonym odpowiednie materiały szkoleniowe, adekwatne do zakresu szkolenia. • Szkolenie powinno zostać przeprowadzone w języku polskim do 14 lutego 2020 w terminie uzgodnionym i zaakceptowanym przez Zamawiającego. 11. Dostarczone oprogramowanie powinno zawierać dostawę licencji umożliwiających pełne działanie wszystkich modułów oprogramowania dostępnych w momencie składania oferty oraz pełne zarządzanie minimum 200 urządzeniami sieci ze wsparciem producenta i dostępem do aktualizacji oprogramowania w ciągu 12 miesięcy od dostawy. W ramach oferty Wykonawcy gwarantowane będą określone poniżej warunki: • licencja wieczysta na dostarczone oprogramowanie, • moduł sieciowy dla nielimitowanej ilości monitorowanych urządzeń, • możliwość instalacji wielu konsol administracyjnych, • możliwość przedłużenia Umowy Serwisowej na kolejne 12 miesięcy w cenie nie przekraczającej 20% wartości licencji przy zachowaniu ciągłości usługi, • dostępność oprogramowania w dowolnej konfiguracji modułowej (funkcjonalnej) według		

		rzeczywistych indywidualnych potrzeb użytkownika, • możliwość zwiększenia liczby zarządzanych stacji roboczych w ramach jednej licencji w dowolnym czasie.		

*do wypełnienia przez Wykonawcę, zapisy „Tak", „Zgodnie", czy „Spełnia" „Jak obok" nie będą akceptowane, należy podać precyzyjnie rzeczywisty oferowany parametr. Wypełniają Wykonawcy składający ofertę na dany pakiet.

_____ dnia __ __ 2019 rok

_____

(pieczęć i podpis)

Pakiet 3: Dostawa urządzenia – serwer NAS z dyskami:

__	**Parametry Zamawiającego**		**Oferowane przez Wykonawcę parametry***	
Lp.	**Przedmiot zamówienia**	**Opis - Parametry techniczne**	**Przedmiot zamówienia (nazwa, producent, numer katalogowy***	**Parametry techniczne***
1.	Serwer NAS	**Urządzenie powinno spełniać wyspecyfikowane minimalne parametry:** Specyfikacja sprzętowa 1. Obudowa urządzenia wysokości 1U do montażu stelażowego. W komplecie wszystkie elementy montażowe do instalacji w szafie rack 19". Wskaźniki LED front: HDD 1–4, stan, USB, LAN 2. Procesor czterordzeniowy taktowany zegarem min. 2,0 GHz. Wykonany w architekturze 64-bit x86. Koprocesor arytmetyczny FPU. Wsparcie mechanizmu szyfrowania AES-NI z akceleracją sprzętową.		

		3. Pamięć systemowa: 4GB SO-DIMM DDR3L (1 x 4GB). Maksymalna pojemność pamięci: 16GB (2 x 8GB). Pamięć flash: 512MB (ochrona systemu operacyjnego przed podwójnym rozruchem) 4. Wnęka dysków: 4 x 3.5-inch SATA 6Gb/s, 3Gb/s Kompatybilność dysków: 3,5-calowe dyski twarde SATA; 2,5-calowe dyski twarde SATA; 2,5-calowe dyski SSD SATA. Możliwa wymiana dysków podczas pracy urządzenia. 5. Port Gigabit sieci Ethernet (RJ45): 4 szt. Port 10 Gigabit sieci Ethernet: 1 x 10GBASE-T (10G/5G/2,5G/1G/100M) - fabrycznie zainstalowana karta PCIe w gnieździe Slot 1: PCIe Gen 2 x4. Obsługa ramek Jumbo. 3 x Port USB 2.0 2 x Port USB 3.0 Opcjonalny Port USB 3.1 Gen 2 (10 Gb/s) na karci rozszerzeń w gnieździe PCIe. 6. Zasilacze nadmiarowe: 2 szt. 250 W, wejście: 110–240 V, 50–60 Hz, 5 A Specyfikacja oprogramowania 7. System operacyjny przygotowany przez producenta urządzenia na bazie LINUX. Obsługiwane systemy operacyjne: Linux i UNIX, Microsoft Windows 7, 8, and 10, Microsoft Windows Server 2003, 2008 R2, 2012, 2012 R2 and 2016. 8. Obsługiwane przeglądarki: Google Chrome, Microsoft Internet Explorer 10 lub nowszy, Mozilla Firefox.		

		9. Wspierany język interfejsu obsługi systemu operacyjnego: Polski. 10. Obsługiwane systemy plików: wewnętrzny zasób dyskowy (EXT4), zewnętrzny zasób dyskowy (EXT3, EXT4, NTFS, FAT32, HFS+, and exFAT) 11. Sieć i przełącznik wirtualny: TCP/IP: Dual stack (IPv4 and IPv6), Jumbo frame (failover, multi-IP settings, port trunking/NIC teaming), DHCP server and client, USB Wi-Fi adapter, Virtual switch WirelessAP Station 12. Zabezpieczenia: Zabezpieczenie dostępu sieciowego z autoblokadą (SSH, Telnet, HTTP(S), FTP, CIFS/SMB, and AFP), Kontrola dostępu udostępnionych folderów (CIFS/SMB), szyfrowanie AES 256-bit woluminów i udostępnionych folderów (FIPS), 256-bit szyfrowanie dysków zewnętrznych (AES), Import i rejestrowanie certyfikatów SSL, natychmiastowe powiadamianie email, SMS, push service, audio, i LCD panel z dwustopniową weryfikacją. 13. Zarządzanie pamięcią masową: • Monitorowanie wykorzystania przestrzeni dyskowej, • Elastyczne woluminy i jednostki LUN z udostępnianiem i odzyskiwaniem przestrzeni, • Obsługiwane typy macierzy RAID: RAID 0, 1, 5, 6, 10, JBOD, Single, • RAID hot spare i globalny hot spare,		

		• Dostosowywanie szybkości odbudowywania macierzy RAID, • Zaawansowane bezpieczne usuwanie danych, • Pule pamięci, • Technologia Qtier (automatyczne tworzenie warstw magazynowych), • Migawki, • Rozszerzenie wolumenu online, • Rozszerzenie puli pamięci online, • Zwiększanie pojemności macierzy RAID online, • Migracja online RAID, • Migracja danych SMART, • Rozszerzenie pamięci za pomocą jednostek rozszerzeń producenta urządzenia, • Roaming w obudowie JBOD • Pamięć podręczna SSD tylko do odczytu lub do odczytu i zapisu • Zły skan bloku i test S.M.A.R.T na dysku twardym. • Odzyskiwanie złych bloków i odzyskiwanie RAID • Obsługa bitmap 14. iSCSI: • iSCSI targets z wieloma jednostkami LUN, • Mapowanie i maskowanie jednostek LUN, • Zwiększenie pojemności jednostek LUN online • Stała rezerwacja SPC-3 15. Zarządzanie energią: • Wake-on-LAN • Tryb gotowości dla dysków wewnętrznych • Zaplanowane włączanie i wyłączanie		

		• Automatyczne włączanie po odzyskaniu zasilania • Obsługa USB i sieciowego UPS z zarządzaniem SNMP 16. Zarządzanie prawami dostępu: • Tworzenie wielu użytkowników • Importowanie i eksportowanie danych użytkownika • Zarządzanie przydziałami użytkowników • Lokalna kontrola dostępu użytkownika (AFP, CIFS / SMB, FTP i WebDAV) 17. Uwierzytelnianie domeny: • Obsługa Microsoft Active Directory (AD) i kontrolera domeny • Serwer i klient LDAP • Logowanie użytkownika domeny (AFP, CIFS / SMB, FTP i File Station) 18. Usługi chmurowe: • Darmowa rejestracja nazwy hosta (DDNS) • Opcjonalne certyfikaty SSL (DDNS) producenta urządzenia • Automatyczna konfiguracja routera za pomocą UPnP • Internetowy menedżer plików z szyfrowaniem HTTPS 2048-bit • CloudLink do zdalnego dostępu bez skomplikowanej konfiguracji routera 19. Usługi synchronizacji: • Synchronizacja plików na wielu urządzeniach z bezpiecznym połączeniem SSL		

		• Selektywna synchronizacja dla określonych folderów lub podfolderów • Foldery zespołu jako centrum plików dla lepszej współpracy Uwaga: Maksymalna liczba zadań synchronizacji wynosi 32. • Udostępnianie plików za pomocą linków e-mail 20. Monitor zasobów: • Monitorowanie zasobów systemu NAS, takich jak procesor, pamięć i sieć • Monitorowanie zasobów pamięci NAS, takich jak woluminy, RAID i aktywność dysku • Monitorowanie wykorzystania zasobów aplikacji NAS • Tworzenie dodatkowej przestrzeni wymiany po zainstalowaniu dysków SSD 21. Wsparcie: • Zgłaszanie problemów zespołowi wsparcia producenta urządzenia z automatycznym gromadzeniem informacji o systemie • Zdalne połączenie między inżynierami wsparcia producenta urządzenia a NAS w celu rozwiązania problemu (za zgodą użytkownika) 22. Administracja sieci: • Zarządzanie systemem z wieloma oknami i wieloma zadaniami • Inteligentny pasek narzędzi i pulpit do wyświetlania statusu systemu • Dynamiczny DNS (DDNS) • Wersje 2 i 3 SNMP • Monitor zasobów • Kosz sieci		

		• Kompleksowe dzienniki (zdarzenia i połączenia) • Serwer i klient Syslog • Tworzenie kopii zapasowych i przywracanie ustawień systemu • Aplikacja mobilna do zdalnego monitorowania i zarządzania systemem 23. Serwer plików: • Udostępnianie plików w systemach Windows, Mac i Linux / UNIX • Sieć Microsoft • Windows ACL • Zaawansowane uprawnienia do folderów (AFP, CIFS / SMB i FTP) • Agregacja folderów współdzielonych (CIFS / SMB) 24. PrintServer: • Maksymalna liczba drukarek: 3 • Obsługuje protokół drukowania internetowego • Wyświetlanie i zarządzanie zadaniami drukowania • Kontrola uprawnień na podstawie adresu IP i nazwy domeny 25. FTP Server: • FTP przez SSL / TLS (jawnie) • Obsługa FXP 26. Manager plików: • Montaż napędu w chmurze dla Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive dla Firm, HiDrive, Amazon Cloud Drive, Yandex Disk and Box		

		• Zdalne montowanie folderów współdzielonych (CIFS / SMB, FTP i WebDAV) • Przeglądanie dokumentów przy użyciu Office Online, Dokumentów Google i rozszerzenia Chrome • Edycja plików Microsoft Office przy użyciu Dokumentów, Arkuszy i Prezentacji Google 27. Backup i archiwizacja: • Automatyczne archiwizowanie • Funkcja przepisu • Archiwizacja przez iSCSI, USB, DVD i zdalny NAS • Kopia zapasowa w chmurze do Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Openstack Swift, WebDAV i HKBN • Synchronizacja magazynu w chmurze z Microsoft OneDrive, Dyskiem Google, Dropbox, Amazon Drive, Yandex Disk, Box, hubiC, BackBlaze B2, Amazon S3 i HiDrive • Serwer i klient RTRR z kontrolą przepustowości • Serwer Rsync z kontrolą przepustowości pobierania 28. Zarządzanie zdjęciami: • Organizacja zdjęć według miniatury, listy, osi czasu lub folderu • Albumy wirtualne i inteligentne • Kontrola ważności udostępniania albumów • Oznaczanie zdjęć tekstem, kolorami i ocenami • Pokazy slajdów z muzyką w tle i efektami przejścia		

		• Geotagowanie zdjęć i wyświetlanie w Mapach Google • Tworzenie kopii zapasowej i przywracanie konfiguracji albumu • Zaawansowane uprawnienia do folderów • Wsparcie dla użytkowników domeny • Photo manager: obsługuje wykrywanie twarzy i PDF do obrazu • Aplikacja mobilna do przeglądania i udostępniania online • wideo online 29. Wyszukiwanie: • Wyszukiwanie pełnotekstowe • Dystrybucja danych za pomocą wykresu słupkowego • Podgląd zdjęć, muzyki, filmów, plików PDF, Gmaila i innych • Zaawansowane operatory wyszukiwania i zakres wyszukiwania • Dostosowane filtry wyszukiwania z włączonymi lub wyłączonymi warunkami • Sugestia powiązanych plików w przeglądarce • Wyszukaj rozszerzenie Chrome 30. DLNA: • Obsługa telewizorów DLNA / UPnP i odtwarzaczy takich jak PlayStation 4 i Xbox One • Obsługa pliku indeksującego CUE dla APE i FLAC 31. Inne funkcje: • Lokalizacja NAS w tej samej sieci lokalnej • Montaż folderu współdzielonego NAS		

		• Podstawowa konfiguracja ustawień (oprogramowanie układowe, serwer SMTP i ustawienia sieciowe) • Storage Plug & Connect (tylko Windows) • Przesyłanie multimediów (tylko Windows) 32. W komplecie: 2 x kable Ethernet, 2 x kable zasilające, komplet śrub do mocowania dysków HDD 3,5", komplet śrub do mocowania dysków HDD 2,5".		
2.	Dyski HDD przeznaczone do pracy z powyższym serwerem NAS	Dyski powinny spełniać poniżej wyspecyfikowane minimalne parametry: Dedykowane do pracy ciągłej w NAS. Obecne na liście kompatybilności producenta NAS. – wszystkie dyski jednakowe pod względem producenta, modelu, firmware oraz minimalnych danych technicznych przedstawionych poniżej: Pojemność – 10 TB Interfejs – SATA III (600) Pamięć podręczna – 256 MB Prędkość obrotowa – 7 200 obr/min. Średnia prędkość odczytu – 240 MB/s Średni czas między uszkodzeniami – 1000000 h Stopa błędów przy odczycie – 1:10E15		

*do wypełnienia przez Wykonawcę, zapisy „Tak", „Zgodnie", czy „Spełnia" „Jak obok" nie będą akceptowane, należy podać precyzyjnie rzeczywisty oferowany parametr. Wypełniają Wykonawcy składający ofertę na dany pakiet.

_____ dnia __ __ 2019 rok

_____

(pieczęć i podpis)

Pakiet 4: Dostawa akcesoriów komputerowych:

___	Parametry Zamawiającego		Oferowane przez Wykonawcę parametry*	
Lp.	**Przedmiot zamówienia**	**Opis - Parametry techniczne**	**Przedmiot zamówienia (nazwa, producent, numer katalogowy***	**Parametry techniczne***
1.	Szafa z wyposażeniem dla serwerów i urządzeń teletechnicznych	Szafa powinna spełniać poniżej wyspecyfikowane parametry: Możliwość instalowania urządzeń teleinformatycznych i telekomunikacyjnych zgodnych ze standardem 19", Wymiary 42U, 800x1000 mm. Drzwi perforowane. Materiał – blacha stalowa. Otwory kablowe o szerokości 71 mm w płycie dolnej i górnej, pozwalające na wprowadzanie kabli zasilających z wtyczkami trójfazowymi. Wszystkie otwory w płycie dolnej i górnej zamknięte wyłamywanymi zaślepkami. Numeracja jednostek U na belkach nośnych. Minimalny kąt otwarcia drzwi przednich 170°. Możliwość zmiany kierunku otwierania drzwi. Możliwość ustawienia szafy bez stopek bezpośrednio na podłodze (brak wystających elementów pod szafą). Dopuszczalne obciążenie – nie mniej niż 800 kg dla szafy ustawionej na stopkach, cokole lub bezpośrednio na podłodze. Poniżej wyszczególniono wymagany osprzęt: • Panel wentylacyjny minimum 2 wentylatory. • Listwa zasilająca 19" gniazdo 9 x CEE 7/5 wtyk IEC320 C14, min. obciążenie 3500W, prąd znamionowy listwy min. 16A – 2 szt.		

		• Półka min. 650mm gł. 4 pkt. Mocowania – 1 szt. W ramach dostawy Wykonawca dostarczy szafę do Zakładu Higieny Weterynaryjnej w Warszawie Oddział Terenowy w Ostrołęce ul. Składowa 8a i na miejscu zmontuje oraz ustawi we wskazanej przez Informatyka Zamawiającego lokalizacji. Osprzęt powinien być zamontowany do szafy w konfiguracji uzgodnionej z Informatykiem WIW w Siedlcach.		
2.	Czytnik kodów kreskowych	Laserowy ręczny czytnik kodów kreskowych USB z dodatkową podstawą w celu umożliwienia ustawienia go na biurku i możliwością automatycznego odczytu kodów po wykryciu zbliżonego dokumentu bez konieczności wciskania przycisku w czytniku		
3.	Podkładka żelowa pod myszkę	Podkładka pod myszkę optyczną o parametrach: - pokryta od góry w całości jednorodną tkaniną w kolorze szarym lub grafitowym - zintegrowana żelowa poduszka pod nadgarstek - od spodu pod całością podkładki jednorodna gumowa lub gumo-podobna powłoka w kolorze czarnym zapobiegająca przemieszczaniu podkładki na biurku		

*do wypełnienia przez Wykonawcę, zapisy „Tak", „Zgodnie", czy „Spełnia" „Jak obok" nie będą akceptowane, należy podać precyzyjnie rzeczywisty oferowany parametr. Wypełniają Wykonawcy składający ofertę na dany pakiet.

_____ dnia __ __ 2019 rok

_____

(pieczęć i podpis)

Pakiet 5: Dostawa zasilaczy awaryjnych – UPS:

___	Parametry Zamawiającego		Oferowane przez Wykonawcę parametry*	
Lp.	**Przedmiot zamówienia**	**Opis - Parametry techniczne**	**Przedmiot zamówienia (nazwa, producent, numer katalogowy***	**Parametry techniczne***
1.	UPS - Zasilacz awaryjny	Zasilacz awaryjny powinien spełniać poniżej wyspecyfikowane minimalne parametry: • Interfejs: USB 2.0 (minimum jeden) • Moc pozorna: min. 3000 VA • Moc skuteczna: min. 2700 W • Liczba gniazd: min. 10 gniazd • Napięcie zasilania / zasilacza: 230 V • Topologia: online • Rodzaj wtyczki zasilającej: Typ E lub F • Certyfikaty: CE, CE Mark, EAC, EN/IEC 62040-1, EN/IEC 62040-2, RCM, VDE, REACH • Napięcie wejściowe: 230V • Maks. zniekształcenia harmoniczne THDi (mniej niż): 2 % • Obsługiwane zakresy częstotliwości: 50-60 Hz • Kształt przebiegu wyjściowego: sinusoida • Minimalna pojemność Akumulatora, VAh: 500 • Typ akumulatora: Bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu		

		• Typ obudowy: tower (stojąca) • Panel sterowania Wielofunkcyjna konsola sterownicza i informacyjna z wyświetlaczem • Alarm: Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia.		

*do wypełnienia przez Wykonawcę, zapisy „Tak", „Zgodnie", czy „Spełnia" „Jak obok" nie będą akceptowane, należy podać precyzyjnie rzeczywisty oferowany parametr. Wypełniają Wykonawcy składający ofertę na dany pakiet.

_____ dnia __ __ 2019 rok

_____

(pieczęć i podpis)

Pakiet 6: Dostawa urządzeń firewall:

___	**Parametry Zamawiającego**		**Oferowane przez Wykonawcę parametry***	
Lp.	**Przedmiot zamówienia**	**Opis - Parametry techniczne**	**Przedmiot zamówienia (nazwa, producent, numer katalogowy***	**Parametry techniczne***
1.	Urządzenie zabezpieczenia brzegu sieci komputerowej - firewall	Dostawa urządzenia nowego i nie regenerowanego, o nie gorszych parametrach technicznych niż wskazano poniżej: **OBSŁUGA SIECI** 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.		

		ZAPORA KORPORACYJNA (Firewall) 2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 4. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 5. Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 7. Administrator powinien mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP		

		(wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). **INTRUSION PREVENTION SYSTEM (IPS)** 10. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 11. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 12. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 13. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 14. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. 15. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 16. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. **KSZTAŁTOWANIE PASMA (Traffic Shapping)** 17. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 18. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w		

		odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 19. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 20. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. **OCHRONA ANTYWIRUSOWA** 21. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 22. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 23. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 24. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. **OCHRONA ANTYSPAM** 25. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 26. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner.		

		27. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 28. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. **WIRTUALNE SIECI PRYWANTE (VPN)** 29. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 30. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 31. SSL VPN musi działać w trybach Tunel i Portal. 32. W ramach funkcji SSL VPN producent powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 33. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 34. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 35. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. **FILTR DOSTĘPU DO STRON WWW** 36. Urządzenie ma posiadać wbudowany filtr URL. 37. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.		

		38. Administrator musi mieć możliwość dodawania własnych kategorii URL. 39. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 40. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 41. Administrator powinien posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 42. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 43. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 44. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 45. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 46. Urządzenie powinno posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 47. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. **UWIERZYTELNIANIE** 48. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:		

		a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 49. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 50. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 51. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 52. Co najmniej jedna z metod transparentnej autoryzacji nie powinna wymagać instalacji dedykowanego agenta. 53. Autoryzacja użytkowników z Microsoft Active Directory nie powinna wymagać modyfikacji schematu domeny. **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)** 54. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 55. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia.		

		56. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 57. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 58. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 59. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 60. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 61. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 62. Rozwiązanie powinno wspierać technologię Link Aggregation. **POZOSTAŁE ROZWIĄZANIA USŁUGI I FUNKCJE** 63. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 64. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 65. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 66. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS		

		67. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 68. Urządzenie musi posiadać usługę DNS Proxy. **ADMINISTRACJA URZĄDZENIEM** 69. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. 70. Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w języku polskim. 71. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową, a komunikacja musi być zabezpieczona za pomocą protokołu https. 72. Komunikacja powinna móc odbywać się na porcie innym niż https (443 TCP). 73. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 74. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 75. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 76. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 77. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX.		

		78. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 79. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. **RAPORTOWANIE** 80. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 81. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 82. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 83. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów. 84. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 85. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 86. Dodatkowy system powinien umożliwiać tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy **PARAMETRY SPRZĘTOWE**		

		87. Urządzenie ma być wyposażone w dysk o pojemności co najmniej 250 GB. 88. Liczba portów Ethernet 10/100/1000Mbps – min. 12. 89. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 90. Przepustowość Firewalla – min. 5 Gbps 91. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 3 Gbps. 92. Przepustowość filtrowania Antywirusowego – min. 850 Mbps 93. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1 Gbps. 94. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 500 95. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 100 96. Obsługa min. VLAN 256 97. Liczba równoczesnych sesji - min. 500 000 i nie mniej niż 20 000 nowych sesji/sekundę. 98. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 99. Urządzenie powinno być nielimitowane na użytkowników. 100. Każde z urządzeń musi mieć możliwość pracy jako drugie w klastrze HA dwóch urządzeń niniejszej specyfikacji, działających co najmniej w trybie Active/Passive 101. Wykonawca przy udziale pracownika Zamawiającego przeprowadzi wymianę dwóch urządzeń NETASQ U 150S zainstalowanych w lokalizacji: siedziba główna Wojewódzkiego		

		Inspektoratu Weterynarii z/s w Siedlcach, ul. Kazimierzowska 29, 08-110 Siedlce. Wykonawca przeniesie konfigurację jednego obecnego urządzenia na dostarczone urządzenie, drugie urządzenie skonfiguruje do pracy jako drugie w klastrze HA dwóch urządzeń niniejszej specyfikacji. Proces przenoszenia przez Wykonawcę konfiguracji i produkcyjne uruchomienie transmisji danych na dostarczanym urządzeniu nie może wpływać na utrzymanie ciągłości transmisji danych w trakcie godzin pracy. Wymieniane urządzenia pozostaną u Zamawiającego. 102. Do urządzeń powinny być załączone min. 3 miesięczne licencje dla następujących usług urządzenia: Firewall z mechanizmem Intrusion Prevention System, WIRTUALNE SIECI PRYWANTE (VPN), FILTR DOSTĘPU DO STRON WWW, OCHRONA ANTYWIRUSOWA, OCHRONA ANTYSPAM. Zakres funkcjonalny wymienionych usług urządzenia w okresie realizacji licencji czasowych powinien być zgodny i nie mniejszy niż określa niniejsza specyfikacja.		
2.	Urządzenie zabezpieczenia brzegu sieci komputerowej - firewall	Dostawa urządzenia nowego i nie regenerowanego, o nie gorszych parametrach technicznych niż wskazano poniżej: **OBSŁUGA SIECI** 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.		

		ZAPORA KORPORACYJNA (Firewall) 2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 4. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 5. Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 7. Administrator powinien mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP		

		(wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). **INTRUSION PREVENTION SYSTEM (IPS)** 10. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 11. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 12. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 13. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 14. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. 15. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 16. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. **KSZTAŁTOWANIE PASMA (Traffic Shapping)** 17. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 18. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w		

		odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 19. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 20. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. **OCHRONA ANTYWIRUSOWA** 21. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 22. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 23. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 24. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. **OCHRONA ANTYSPAM** 25. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 26. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner.		

		27. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 28. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. **WIRTUALNE SIECI PRYWANTE (VPN)** 29. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 30. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 31. SSL VPN musi działać w trybach Tunel i Portal. 32. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 33. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 34. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 35. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. **FILTR DOSTĘPU DO STRON WWW** 36. Urządzenie ma posiadać wbudowany filtr URL. 37. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.		

		38. Administrator musi mieć możliwość dodawania własnych kategorii URL. 39. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 40. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 41. Administrator powinien posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 42. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 43. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 44. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 45. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 46. Urządzenie powinno posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 47. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. **UWIERZYTELNIANIE** 48. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:		

		a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 49. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 50. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 51. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 52. Co najmniej jedna z metod transparentnej autoryzacji nie powinna wymagać instalacji dedykowanego agenta. 53. Autoryzacja użytkowników z Microsoft Active Directory nie powinna wymagać modyfikacji schematu domeny. **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)** 54. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 55. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia.		

		56. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 57. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 58. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 59. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 60. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 61. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. **POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA** 62. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 63. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 64. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 65. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 66. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.		

		67. Urządzenie musi posiadać usługę DNS Proxy. **ADMINISTRACJA URZĄDZENIEM** 68. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. 69. Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w języku polskim. 70. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 71. Komunikacja powinna móc odbywać się na porcie innym niż https (443 TCP). 72. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 73. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 74. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 75. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 76. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 77. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na		

		dedykowany serwer zarządzany przez administratora. 78. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. **RAPORTOWANIE** 79. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 80. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 81. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 82. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. 83. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 84. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 85. Dodatkowy system powinien umożliwiać tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy **PARAMETRY SPRZĘTOWE** 86. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.		

		87. Liczba portów Ethernet 10/100/1000Mbps – min. 8. 88. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 89. Przepustowość Firewalla – min. 3,5 Gbps 90. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 2,4 Gbps. 91. Przepustowość filtrowania Antywirusowego – min. 400 Mbps 92. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 600 Mbps. 93. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100. 94. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. 95. Obsługa min. VLAN 64 96. Liczba równoczesnych sesji - min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę. 97. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 98. Urządzenie powinno być nielimitowane na użytkowników. 99. Urządzenie musi być wyposażone dodatkowo w nośnik pamięci flash o pojemności minimum 64 GB (gwarancja na pamięć min. 12 miesięcy) 100. Wykonawca dostarczy dedykowane rozwiązanie do tworzenia raportów w formie maszyny wirtualnej do zainstalowania w środowisku zamawiającego dla wszystkich urządzeń niniejszej specyfikacji. 101. Wykonawca przy wsparciu pracownika Zamawiającego wymieni urządzenia		

		NETASQ U 70S zainstalowanego w lokalizacji: Zakład Higieny Weterynaryjnej w Warszawie, ul. Lechicka 21, 02-156 Warszawa oraz urządzenia NETASQ U 30S zainstalowanego w lokalizacji: Zakład Higieny Weterynaryjnej w Warszawie Oddział Terenowy w Ostrołęce, ul. Składowa 8A, 07-411 Ostrołęka. Wykonawca przeniesie konfigurację obecnych urządzeń na dostarczone urządzenia. Proces przenoszenia przez Wykonawcę konfiguracji i produkcyjne uruchomienie transmisji danych na dostarczanym urządzeniu nie może wpływać na utrzymanie ciągłości transmisji danych w trakcie godzin pracy. Wymieniane urządzenia pozostaną u Zamawiającego. 102. Do urządzenia powinny być załączone min. 3-miesięczne licencje dla następujących usług urządzenia: Firewall z mechanizmem Intrusion Prevention System, WIRTUALNE SIECI PRYWANTE (VPN), FILTR DOSTĘPU DO STRON WWW, OCHRONA ANTYWIRUSOWA, OCHRONA ANTYSPAM. Zakres funkcjonalny wymienionych usług urządzenia w okresie realizacji licencji czasowych powinien być zgodny i nie mniejszy niż określa niniejsza specyfikacja. Wykonawca przeprowadzi jednodniowe warsztaty techniczne ze wszystkich urządzeń niniejszego pakietu w języku polskim dla dwóch pracowników		

		Zamawiającego w siedzibie i na urządzeniach Wykonawcy w terminie do 31 marca 2020 roku.		

*do wypełnienia przez Wykonawcę, zapisy „Tak", „Zgodnie", czy „Spełnia" „Jak obok" nie będą akceptowane, należy podać precyzyjnie rzeczywisty oferowany parametr. Wypełniają Wykonawcy składający ofertę na dany pakiet.

_____ dnia __ __ 2019 rok

_____

(pieczęć i podpis)

Załącznik nr 6 do SIWZ

Nr sprawy: WIW-AD.272.97.2019

HARMONOGRAM DOSTAW

Pakiet 1: Dostawa urządzeń wielofunkcyjnych

Miejsce realizacji: Dostawa, montaż i uruchumienie urządzeń w Wojewódzkim Inspektoracie Weterynarii z/s w Siedlcach, ul. Kazimierzowska 29, 08-110 Siedlce.

Lp.	Przedmiot zamówienia	Ilość zamawiana	2019 rok
1.	Urządzenia wielofunkcyjne	4 szt.	do dnia 24 grudnia 2019 roku

Pakiet 2: Dostawa oprogramowania do kompleksowego zarządzania zasobami IT

Miejsce realizacji: Dostawa do Wojewódzkiego Inspektoratu Weterynarii z/s w Siedlcach ul. Kazimierzowska 29, 08-110 Siedlce.

Lp.	Przedmiot zamówienia	Ilość zamawiana	2019 rok
1.	Oprogramowanie do kompleksowego zarządzania zasobami IT	1 pakiet	do dnia 24 grudnia 2019 roku

Pakiet 3: Dostawa urządzenia – serwer NAS z dyskami:

Miejsce realizacji: Dostawa do Wojewódzkiego Inspektoratu Weterynarii z/s w Siedlcach ul. Kazimierzowska 29, 08-110 Siedlce.

Lp.	Przedmiot zamówienia	Ilość zamawiana	2019 rok
1.	Serwer NAS	1 szt.	kompletna dostawa do dnia 24 grudnia 2019 roku
2.	Dyski	4 szt.	

Pakiet 4: Dostawa akcesoriów komputerowych:

Miejsce realizacji: Dostawa do Wojewódzkiego Inspektoratu Weterynarii z/s w Siedlcach oraz do ZHW w Warszawie Oddział Terenowy w Ostrołęce, ul. Składowa 8a, 07-410 Ostrołęka.

Lp.	Przedmiot zamówienia	Ilość zamawiana	Miejsce realizacji:	2019 rok do dnia 24 grudnia 2019 roku
1.	Szafa z wyposażeniem dla serwerów i urządzeń teletechnicznych	1 szt.	Zakład Higieny Weterynaryjnej w Warszawie Oddział Terenowy w Ostrołęce ul. Składowa 8a	do dnia 24 grudnia 2019 roku
2.	Czytnik kodów kreskowych	1 szt.	Wojewódzki Inspektorat Weterynarii z/s w Siedlcach	kompletna dostawa do dnia 24 grudnia 2019 roku
3.	Podkładka żelowa pod myszkę	23 szt.		

Pakiet 5: Dostawa zasilaczy awaryjnych UPS:

Miejsce realizacji: Dostawa do Wojewódzkiego Inspektoratu Weterynarii z/s w Siedlcach ul. Kazimierzowska 29, 08-110 Siedlce.

Lp.	Przedmiot zamówienia	Ilość zamawiana	2019 rok
1.	Zasilacze awaryjne - UPS	3 szt.	kompletna dostawa do dnia 24 grudnia 2019 roku

Pakiet 6: Dostawa urządzeń firewall:

Miejsce realizacji: Dostawa i programowanie do Wojewódzkiego Inspektoratu Weterynarii z/s w Siedlcach ul. Kazimierzowska 29, 08-110 Siedlce..

Lp.	Przedmiot zamówienia	Ilość zamawiana	2019 rok
1.	Urządzenie zabezpieczenia brzegu sieci komputerowej – firewall (wyposażone w dysk)	2 szt.	do dnia 24 grudnia 2019 roku
2.	Urządzenie zabezpieczenia brzegu sieci komputerowej – firewall (wyposażone w nośnik pamięci flash)	2 szt.	