POWIAT TATRZAŃSKI

✉ **ul. Chramcówki 15, 34-500 Zakopane**

☎ tel. (+48 18) 20-17-100 🖳 http://www.powiat.tatry.pl
☎ fax (+48 18) 20-17-104 🖳 e-mail: zp@powiat.tatry.pl

Zakopane, dnia 27 kwietnia 2017 roku

ZP.272.5.2017
pyt. i odp. do SIWZ – Nr 1

Wykonawcy Pobierający Materiały Przetargowe SIWZ
Wszyscy

W wyniku otrzymanych pisemnych pytań dotyczących postępowania przetargowego prowadzonego w trybie przetargu nieograniczonego na: **„Wykonanie dostawy wraz z wdrożeniem urządzeń i oprogramowania zwiększających bezpieczeństwo sieci oraz infrastruktury serwerowej – część 1 dla potrzeb Starostwa Powiatowego w Zakopanem”** działając na podstawie art. 38 ust. 2 i ust. 4 ustawy z dnia 29 stycznia 2004 roku – Prawo zamówień publicznych (j.t. Dz. U. z dnia 22 grudnia 2015 roku, poz. 2164 ze zm.), przesyłam Państwu treść pisemnych pytań, odpowiedzi związaną z udzielonymi wyjaśnieniami na zadane pytania oraz treść modyfikacji, zmian zapisów przedmiotowej Specyfikacji Istotnych Warunków Zamówienia.

I. Pytania i odpowiedzi do SIWZ:

Działając na podstawie art. 38 ust. 2 i ust. 4 wyżej cytowanej ustawy, przesyłam Państwu treść pisemnych pytań oraz wyjaśnienia na zadane pytania w związku z przedmiotowym postępowaniem przetargowym:

Pytania dotyczące oprogramowania: Wszystkie komputery z pakietu 3 i 4.

1. **Pytanie 1**
   Czy Zamawiający wymaga fabrycznie nowego systemu operacyjnego, nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu?
   Odpowiedź: Zamawiający informuje i wyjaśnia, że w zakresie opisu przedmiotu zamówienia poszczególnych komponentów składowych Pakietów Nr 3 i Nr 4 został postawiony warunek w postaci wymagania, aby dostarczony przedmiot zamówienia był w stanie cyt. „fabrycznie nowy”. Należy przez to rozumieć, iż poszczególne elementy składowe przedmiotu zamówienia w tym np. wskazany w pytaniu system operacyjny również był fabrycznie nowy. Mając na uwadze powyższe należy stwierdzić, że dostarczony system operacyjny ma być nowy, wcześniej nieużywany oraz nieaktywowany nigdy wcześniej na innym urządzeniu.

2. **Pytanie 2**

Czy Zamawiający wymaga by oprogramowanie systemowe było fabrycznie zainstalowane przez producenta komputera?

Odpowiedź: Zamawiający informuje i wyjaśnia, że nie stawia takiego wymagania jako warunek uczestnictwa w niniejszym postępowaniu. Ponadto zamawiający informuje, że wykonawca jest zobowiązany dostarczyć kompletny przedmiot zamówienia w tym z zainstalowanym oprogramowaniem systemowym, które musi posiadać wszelkie atrybuty legalności.

3. **Pytanie 3**

Czy Zamawiający wymaga aby oprogramowanie było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności np. certyfikatami autentyczności (tzw. COA)?

Odpowiedź: Zamawiający informuje i wyjaśnia, że dostarczone oprogramowanie będące elementem przedmiotu zamówienia (tj. system operacyjny, oprogramowanie biurowe, itp.) musi posiadać wszelkie atrybuty legalności w zależności od oprogramowania, poświadczające legalność dostarczonego oprogramowania.

4. **Pytanie 4**

Czy w momencie odbioru towaru Zamawiający przewiduje zastosowanie procedury sprawdzającej legalność zainstalowanego oprogramowania? W jaki sposób będzie przebiegała ta procedura?

Odpowiedź: Zamawiający informuje i wyjaśnia, że podczas procedury odbioru przedmiotu zamówienia będzie dokonana weryfikacja parametrów dostarczonego przedmiotu zamówienia z wymogami określonymi w szczegółowych opisach przedmiotu zamówienia (OPZ). Oczywistym jest fakt, że zamawiający w celu zachowania zasad uczciwej konkurencji i równego traktowania wykonawców jak również należytego wydatkowania środków publicznych, dokona weryfikacji legalności dostarczonego oprogramowania według wszelkich dostępnych metod i środków (np. oświadczenie wykonawcy o spełnieniu wymogów OPZ złożone w formularzu ofertowym, weryfikacja atrybutów legalności, weryfikacja poprzez stronę producenta sprzętu, weryfikacja licencji u producenta dostarczanego oprogramowania, itp.). Wykonawca powinien mieć świadomość, że ciąży na nim odpowiedzialność za dostarczenie oprogramowania pochodzącego z nielegalnego kanału dystrybucji.

5. **Pytanie 5**

Czy zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów komputerowych u Producenta oprogramowania jako elementu procedury odbioru?

Odpowiedź: Zamawiający informuje i wyjaśnia, że jednym z elementów weryfikacji legalności dostarczonego oprogramowania będzie jego weryfikacja u producenta, jak również inne metody określone w odpowiedzi na pytanie nr 4 niniejszego pisma.

II.

6. **W Załączniku nr 7 do SIWZ „Opis Przedmiotu Zamówienia. Pakiet Nr 2. Oprogramowanie zwiększające bezpieczeństwo sieci" w rozdziale „Dokumentacja powykonawcza" (str. 112 SIWZ) mamy zapis: „Dodatkowo w zakresie zwiększenia bezpieczeństwa sieciowego Zamawiający otrzyma dokumentację certyfikowaną, voucher z zakresu Cobit Foundation oraz ITIL Foundation". Prosimy w związku z tym o wyjaśnienie:**
   a) co Zamawiający rozumie przez „dokumentację certyfikowaną"?
   b) czy Zamawiający wymaga dostarczenia vouchera na szkolenie z zakresu Cobit Foundation oraz ITIL Foundation?
   c) w przypadku odpowiedzi twierdzącej na pytanie b) – czy Zamawiający oczekuje dostarczenia dwóch voucherów: jednego na szkolenie Cobit Foundation i drugiego – na szkolenie ITIL Foundation?

   Odpowiedź: Zamawiający informuje i wyjaśnia, że wymaga w zakresie zwiększenia bezpieczeństwa sieciowego dostawy dokumentacji certyfikowanej przez którą należy rozumieć dokumentację, materiały opisujące zastosowanie dwóch metodyk i standardów (Cobbit, ITIL) zarządzania środowiskiem informatycznym w organizacji oraz zapoznanie przestawiciela Zamawiającego z niniejszymi metodykami. Dodatkowo zamawiający informuje, że w zakresie pkt. b i c pytania potwierdza możliwość spełnienia zapisów SIWZ w przedstawiony sposób.

III.

7. **W „Wymaganiach minimalnych dla poszczególnych komponentów i oprogramowania" dotyczących pakietu oprogramowania antywirusowego znajduje się zapis: „Program ma mieć moduł skanujący protokoły POP3, SMTP, IMAP niezależny od klienta pocztowego".**
   Ponieważ taki wymóg może ograniczać konkurencyjność ze względu na fakt, iż warunek ten jest spełniony w przypadku konkretnego rozwiązania antywirusowego, zaś szereg programów antywirusowych posiada moduły współpracujące z ogromną większością popularnych klientów poczty elektronicznej, co powinno w pełni zaspokoić potrzeby Zamawiającego w tym zakresie, prosimy uprzejmie o usunięcie przedmiotowego zapisu.

   Odpowiedź: Zamawiający informuje i wyjaśnia, że postanawia dokonać modyfikacji zamian zapisów szczegółowego opisu przedmiotu zamówienia „OPZ" stanowiącego załącznik nr 7 do przedmiotowej SIWZ w zakresie części III dotyczącej pakietu oprogramowania antywirusowego, pozycja 3 tabeli (ogólne właściwości oprogramowania antywirusowego), która otrzymuje nowe brzmienie:

Pakiet oprogramowania antywirusowego		
Lp.	**Parametr**	**Minimalne wymagania**
1	2	3
3	Ogólne właściwości oprogramowania	- Oprogramowanie antywirusowe musi być dostępne w pakietach instalacyjnych dla stacji roboczych oraz serwerów. Dostarczane klucze licencyjne muszą pozwalać na aktywowanie

	antywirusowego	oprogramowania przeznaczonego do ochrony stacji roboczych oraz serwerów. - Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami, ransomware i innymi potencjalnie niebezpiecznymi programami. - Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony. - Program ma mieć możliwość skanowania i klasyfikowania plików oraz odsyłaczy do zasobów sieciowych na podstawie informacji gromadzonych w oparciu o dane dostarczane przez producenta. - Program powinien chronić przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX). - Program ma mieć funkcję wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz innych narzędzi hakerskich. **- Program ma mieć moduł skanujący pocztę przychodzącą i wychodzącą dla klienta poczty elektronicznej minimum Microsoft Office Outlook, który to program jest używany przez Zamawiającego.** - Wbudowany moduł skanujący ruch HTTP w ma działać czasie rzeczywistym niezależnie od wykorzystywanej przez użytkowników przeglądarki WWW. - Program ma posiadać wbudowany moduł wyszukiwania heurystycznego - Program ma umożliwiać ochronę przed niebezpiecznymi rodzajami aktywności sieciowej oraz umożliwiać tworzenie reguł wykluczających dla określonych adresów/zakresów IP. - Program ma umożliwiać centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym za pośrednictwem modułu serwera oraz dostarczonego oprogramowania konsoli administratora. - Możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych. - Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. - Możliwość tworzenia list zaufanych procesów, dla których nie będzie monitorowana aktywność plikowa, aktywność aplikacji, nie będą dziedziczone ograniczenia nadrzędnego procesu, nie będzie monitorowana aktywność aplikacji potomnych, dostęp do rejestru oraz ruch sieciowy.

W związku z powyższym ulega modyfikacji wzór formularza oferty przetargowej w zakresie Pakietu Nr 2 (załącznik nr 1 do SIWZ) oraz szczegółowy opis przedmiotu zamówienia „OPZ" (załącznik nr 7 do SIWZ), patrz część II niniejszego pisma – Modyfikacja zapisów SIWZ.

IV.

8. Pytanie 1:

W Specyfikacji Istotnych Warunków Zamówienia, Pakiet nr 1, sekcja „Modernizacja sieci LAN (przełączniki 10Gbps i 1Gbps)", punkt 8, parametr „Okablowanie" Zamawiający definiuje:

„Wykonawca dostarczy komplet kabli połączeniowych w szczególności:

kable statkujące - DAC, wkładki światłowodowe, krosowe światłowodowe oraz kable zasilające, itp.. Stackowanie przełączników jedynie przy użyciu kablami DAC lub światłowodowymi. Należy połączyć 3 punkty dystrybucyjne redundatnymi połączeniami SFP+ 10 Gb/s z przełącznikami rdzeniowymi w serwerowni głównej"

Prosimy o udzielenie informacji na temat rodzaju i długości zastosowanego medium połączeniowego, pomiędzy stackami przełączników dostępowych, a przełącznikami

rdzeniowymi oraz podanie informacji na temat złączy zainstalowanych w patchpanelach światłowodowych, czy są typu LC lub SC.
Powyższa informacja jest istotna ze względu na potrzebę dobrania właściwego rodzaju wkładek SFP+.

Odpowiedź: Zamawiający informuje i wyjaśnia, że medium połączeniowe pomiędzy stackami przełączników dostępowych a przełącznikami rdzeniowymi to: światłowód wielomodowy FIBRAIN typ MM 50/125 OM3 LSOH, maksymalny odcinek pomiędzy serwerownią zapasową a serwerownią główną to około 200 m. Natomiast złącza w patchpanelach światłowodowych przewidziane są typu LC.

9. **Pytanie 2:**
W Specyfikacji Istotnych Warunków Zamówienia, Pakiet nr 1 , sekcja „Przełącznik rdzeniowy (switch) 10G", punkt 8, parametr „Okablowanie" Zamawiający definiuje:
Wykonawca dostarczy kable przyłączeniowe do połączenia oferowanego urządzenia z dostarczanymi urządzeniami sieciowymi w szczególności: kable do statkowania kable krosowe światłowodowe wkładki światłowodowe oraz kable zasilające. Dodatkowo przełącznik powinien zapewniać podłączenie serwerów, np. powinien mięć zainstalowane przynajmniej wkładki 4 szt. 1 GbE T/przełącznik oraz 4 szt. 10 GbE SFP+/przełącznik.
Prosimy o udzielenie informacji na temat rodzaju medium (wielomodowe, jednomodowe) dla wkładek SFP+ oraz długości medium pomiędzy przełącznikiem, a poszczególnymi serwerami.
Powyższa informacja jest istotna ze względu na potrzebę dobrania właściwego rodzaju wkładek SFP+ np. np. SR czy LR.
Czy w wypadku wskazania odległości pomiędzy serwerami, a przełącznikami rdzeniowymi poniżej 5m, Zamawiający dopuści jako spełniające SIWZ połączenie wykonane przy pomocy kabli DAC/TWINAX?

Odpowiedź: Zamawiający informuje i wyjaśnia, że przełączniki rdzeniowe 10G są przewidywane do montażu w tej samej szafie RACK co serwery, odległość pomiędzy serwerami, a przełącznikami rdzeniowymi do 5m.
Ponadto zamawiający informuje i wyjaśnia, że postanawia dokonać modyfikacji zamian zapisów szczegółowego opisu przedmiotu zamówienia „OPZ" stanowiącego załącznik nr 6 do przedmiotowej SIWZ w zakresie części IV dotyczącej przełączników rdzeniowych (switch) 10G, pozycja 8 tabeli (okablowanie), która otrzymuje nowe brzmienie:

Przełącznik rdzeniowy (switch) 10G – 2 szt.		
Lp.	**Parametr**	**Minimalne wymagania**
1	2	3
8	Okablowanie:	Wykonawca dostarczy kable przyłączeniowe do połączenia oferowanego urządzenia z dostarczanymi urządzeniami sieciowymi w szczególności: kable do statkowania kable krosowe światłowodowe wkładki światłowodowe oraz kable zasilające. Dodatkowo przełącznik powinien zapewniać podłączenie serwerów, np. powinien mięć zainstalowane przynajmniej wkładki 4 szt. 1 GbE T/przełącznik oraz 4 szt. 10 GbE SFP+ **(dopuszcza się rozwiązanie połączenia za pomocą kabli DAC/TWINAX)**/przełącznik,

W związku z powyższym ulega modyfikacji wzór formularza oferty przetargowej w zakresie Pakietu Nr 1 (załącznik nr 1 do SIWZ) oraz szczegółowy opis przedmiotu zamówienia „OPZ" (załącznik nr 6 do SIWZ), patrz część II niniejszego pisma – Modyfikacja zapisów SIWZ.

10. **Pytanie 3:**
Zamawiający w Specyfikacji Istotnych Warunków Zamówienia w sekcji „Przełącznik rdzeniowy (switch) 10G" w punkcie 8 parametr „Okablowanie" nie wskazał konieczności zapewnienia odpowiednich wkładek dla celów połączenia pomiędzy przełącznikami rdzeniowymi, a urządzeniami UTM.
W Specyfikacji Istotnych Warunków Zamówienia, Pakiet nr 1 , sekcja „Zakup Zestawu UTM (klaster) – ochrona styku Internet/Intranet", punkt 9, parametr „Parametry sieciowe" Zamawiający definiuje:
„Ilość interfejsów sieciowych: minimum 8x 10/100/1000 BaseT interface".
Prosimy o wyjaśnienie, czy do przełączników rdzeniowych maja być dostarczone dodatkowe wkładki 1 GbE T/RJ45 do celów połączenia przełączników rdzeniowych z urządzeniami UTM, oraz jaka ilość takich wkładek ma zostać dostarczona dla każdego przełącznika rdzeniowego.
Odpowiedź: Zamawiający informuje i wyjaśnia, że w szczegółowym opisie przedmiotu zamówienia „OPZ" wymaga dostawy niezbędnego okablowania oraz niezbędnych ilości wkładek do wykonania połączeń pomiędzy urządzeniami zgodnie z określoną koncepcją przedstawioną na załączonym schemacie. Zamawiający informuje, że to rolą wykonawcy jest określenie niezbędnej ilości wkładek dla zapewnienia kompletności i redundantnych połączeń.

V.

11. **Pytanie 1:**
W Specyfikacji Istotnych Warunków Zamówienia, Pakiet nr 1 zamawiający wymaga dostarczenia okablowania i wkładek światłowodowych w tym SFP+ do urządzeń sieciowych.
Prosimy o udzielenie informacji czy wszystkie wkładki powinny być oryginalne i pochodzić od producenta dostarczanych urządzeń sieciowych?
Powyższa informacja jest istotna ze względu m.in. na realizację gwarancji/serwisu ze strony producenta.
Prosimy również o informacje jakiej kategorii patchcordy RJ45 powinny być dostarczone w ww. zadaniu?
Kategoria zastosowany patchcordów RJ45 jest decydująca dla parametrów technicznych realizowanych przy ich wykorzystaniu i może wpłynąć na parametry komunikacyjne osiągane w obrębie infrastruktury sieciowej.
Odpowiedź: Zamawiający informuje i wyjaśnia, że nie narzuca wykonawcom tak szczegółowych wymogów w zakresie opisu przedmiotu zamówienia, nie mających bezpośredniego wpływu na realizację koncepcji zamawiającego. W celu nieograniczania konkurencji zamawiający pozostawia w tym zakresie możliwość doboru odpowiednich materiałów do decyzji wykonawcy. Dobór niniejszych akcesoriów będzie podlegał weryfikacji podczas uzgodnień na

etapie analizy projektu przedwdrożeniowego podczas wykonywania przedmiotu zamówienia. Zaproponowane przez wykonawcę rozwiązanie muszą gwarantować spełnienie minimalnych wymagań jakościowych określonych przez zamawiającego w SIWZ.

VI.

12. W wymaganiach dotyczących „Pakietu Nr 2. Oprogramowanie zwiększające bezpieczeństwo sieci", w drugim obszarze, to jest: „monitorowanie i zarządzanie sprzętem komputerowym oraz użytkownikami" nie dostrzegliśmy informacji o ilości użytkowników/urządzeń, na których oprogramowanie takie powinno być licencjonowane i których powinno obsługiwać.
W związku z powyższym prosimy uprzejmie o podanie liczby urządzeń (unikalnych adresów IP), dla których Zamawiający pragnie nabyć przedmiotowe oprogramowanie.

Odpowiedź: Zamawiający informuje i wyjaśnia, że w zakresie oprogramowania do monitorowania i zarządzania sprzętem komputerowym oraz użytkownikami, dopuszcza możliwość wykonania dostawy oprogramowania zbiorczego na urząd będź dostarczone oprogramowanie musi obsługiwac przynajmniej 130 urządzeń (unikalnych adresów IP) w celu należytego monitorowania bezpieczeństwa urządzeń w sieci urzędu.
Masjąc na uwadze powyższe zamawiający informuje i wyjaśnia, że postanawia dokonać modyfikacji zamian zapisów szczegółowego opisu przedmiotu zamówienia „OPZ" stanowiącego załącznik nr 7 do przedmiotowej SIWZ w zakresie części III dotyczącej oprogramowania monitorowania bezpieczeństwa IT, pozycja 4 tabeli (Monitorowanie i zarządzaniem sprzętem komputerowym oraz użytkownikami), która otrzymuje nowe brzmienie:

Pakietu oprogramowania monitorowania bezpieczeństwa IT		
Lp.	**Parametr**	**Minimalne wymagania**
1	2	3
4	Monitorowanie i zarządzaniem sprzętem komputerowym oraz użytkownikami	Rozwiązanie musi umożliwiać wdrożenie pełnej wymaganej funkcjonalności na platformie wirtualizacyjnej. **Dopuszcza się możliwość wykonania dostawy oprogramowania zbiorczego na urząd bądź dostarczone oprogramowanie musi obsługiwac przynajmniej 130 urządzeń (unikalnych adresów IP) w celu należytego monitorowania bezpieczeństwa urządzeń w sieci urzędu**. Rozwiązanie w niniejszym zakresie musi udostępniać funkcjonalności: Audyt zasobów sprzętowych i oprogramowania: - Lista aplikacji oraz aktualizacji systemu operacyjnego na pojedynczej stacji roboczej (rejestr) - Lista aplikacji oraz aktualizacji systemu operacyjnego na pojedynczej stacji roboczej (skan dysków) - Numery seryjne (klucze) oprogramowania - Informacje o plikach wykonywalnych i wpisach rejestrowych na stacji roboczej - Informacje o plikach multimedialnych (mp3, avi itp.) oraz archiwach zip i ich metadanych (tytuł i autor utworu, zawartość pliku zip) - Ogólne informacje o sprzęcie stacji roboczej - Szczegółowe informacje o sprzęcie stacji roboczej (model, płyta, procesor, pamięć, napędy, karty itp.) - Informacje systemowe (komendy startowe, konta użytkowników, foldery udostępnione, informacje SMART itp.)

		- Audyt inwentaryzacji sprzętu i oprogramowania - Baza wzorców oprogramowania - Zarządzanie licencjami - Historia zmian sprzętu i oprogramowania - Środki Trwałe: baza ewidencji majątku IT (definiowanie własnych typów środków, ich atrybutów oraz wartości, załączniki, import danych z pliku CSV) - Alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych - Skaner inwentaryzacji offline - Skanowanie i drukowanie kodów kreskowych oraz QR

W związku z powyższym ulega modyfikacji wzór formularza oferty przetargowej w zakresie Pakietu Nr 2 (załącznik nr 1 do SIWZ) oraz szczegółowy opis przedmiotu zamówienia „OPZ" (załącznik nr 7 do SIWZ), patrz część II niniejszego pisma – Modyfikacja zapisów SIWZ.

II. Modyfikacja (zmiana) zapisów SIWZ:

Działając na podstawie art. 38 ust. 2 i ust. 4 ustawy z dnia 29 stycznia 2004 roku – Prawo zamówień publicznych, **postanawia się wprowadzić modyfikacje, zmiany zapisów przedmiotowej SIWZ, które stają się jej integralną częścią.** Dokonane zmiany są wiążące dla Wykonawców, którzy pobrali materiały przetargowe (SIWZ).

1. **<u>Ulega zmianie załącznik nr 1 do SIWZ – Formularz oferty przetargowej, który otrzymuje nowe brzmienie:</u>**

   Nowy zmodyfikowany wyjaśnieniami z dnia 27 kwietnia 2017 roku formularz oferty przetargowej, będący załącznikiem nr 1 do SIWZ, jest dołączony do niniejszego pisma w postaci załącznika nr 1.

2. **<u>Ulega zmianie załącznik nr 6 do SIWZ – Opisem przedmiotu zamówienia „OPZ" w zakresie Pakietu Nr 1 – Infrastruktura zwiększająca bezpieczeństwo sieci oraz infrastruktura serwerowa, który otrzymuje nowe brzmienie:</u>**

   Nowy zmodyfikowany wyjaśnieniami z dnia 27 kwietnia 2017 roku Opisem przedmiotu zamówienia „OPZ" w zakresie Pakietu Nr 1, będący załącznikiem nr 6 do SIWZ, jest dołączony do niniejszego pisma w postaci załącznika nr 2.

3. **<u>Ulega zmianie załącznik nr 7 do SIWZ – Opisem przedmiotu zamówienia „OPZ" w zakresie Pakietu Nr 2 – Oprogramowanie zwiększające bezpieczeństwo sieci, który otrzymuje nowe brzmienie:</u>**

   Nowy zmodyfikowany wyjaśnieniami z dnia 27 kwietnia 2017 roku Opisem przedmiotu zamówienia „OPZ" w zakresie Pakietu Nr 2, będący załącznikiem nr 7 do SIWZ, jest dołączony do niniejszego pisma w postaci załącznika nr 3.

W wyniku udzielonych wyjaśnień, a co za tym idzie dokonaniu modyfikacji, zmian zapisów SIWZ przedmiotowego postępowania przetargowego prowadzonego w trybie przetargu nieograniczonego, zamawiający działając zgodnie z postanowieniami art. 38 ust. 4 i ust. 4a w związku z postanowieniami art. 12a cytowanej wyżej ustawy z dnia 29 stycznia 2004 roku – Prawo zamówień publicznych, postanawia dokonać zmiany treści ogłoszenia o zamówieniu (patrz zamawiający niezwłocznie po przekazaniu zmiany treści ogłoszenia o zamówieniu Urzędowi Publikacji Unii Europejskiej zamieszcza informację o zmianach w swojej siedzibie oraz na stronie internetowej) zgodnie z poniższą modyfikacją zapisów SIWZ, a to:

4. <u>Ulega zmianie Punkt 17.9 SIWZ, który otrzymuje nowe brzmienie:</u>

„ Punkt 17.9 SIWZ Ofertę należy złożyć w zamkniętej nieprzeźroczystej kopercie lub opakowaniu, w siedzibie zamawiającego i oznakować w następujący sposób:

Nazwa i adres wykonawcy:
……
……

Starostwo Powiatowe w Zakopanem
ul. Chramcówki 15, 34-500 Zakopane
Dziennik Podawczy

OFERTA PRZETARGOWA
„Wykonanie dostawy wraz z wdrożeniem urządzeń i oprogramowania zwiększających bezpieczeństwo sieci oraz infrastruktury serwerowej – część 1 dla potrzeb Starostwa Powiatowego w Zakopanem”
Nie otwierać przed: 22 maja 2017 roku przed godz. 11:15

5. <u>Ulega zmianie Punkt 18.1 SIWZ, który otrzymuje nowe brzmienie:</u>

„ Punkt 18.1 SIWZ należy złożyć w siedzibie Zamawiającego, tj. Starostwo Powiatowe w Zakopanem, ulica Chramcówki 15, 34-500 Zakopane, pokój numer 1 – Dziennik Podawczy, **do dnia 22 maja 2017 roku**, **do godziny 11:00** i zaadresować zgodnie z opisem przedstawionym w punkcie 17.9 niniejszej SIWZ.”;

6. <u>Ulega zmianie Punkt 18.4 SIWZ, który otrzymuje nowe brzmienie:</u>

„ Punkt 18.4 SIWZ Otwarcie ofert nastąpi w siedzibie Zamawiającego, tj. przy ul. Chramcówki 15, 34-500 Zakopane, pokój nr – sala obrad II p., **w dniu 22 maja 2017 roku o godzinie 11:15.**”.

Załączniki:

1. Załącznik Nr 1 – Zmodyfikowany wzór formularza oferty przetargowej (załącznik Nr 1 do SIWZ),
1. Załącznik Nr 2 – Zmodyfikowany „OPZ” w zakresie Pakietu Nr 1 (załącznik Nr 6 do SIWZ),
2. Załącznik Nr 3 – Zmodyfikowany „OPZ” w zakresie Pakietu Nr 2 (załącznik Nr 7 do SIWZ).

UWAGA !!!

Powyższe zmiany należy uwzględnić w składanej ofercie przetargowej, tj.:

- **składaną ofertę przetargową, należy sporządzić wg nowego zmodyfikowanego wzoru folmularza oferty przetargowej (załącznik nr 1 do niniejszego pisma).**

Z poważaniem:

STAROSTA TATRZAŃSKI

mgr inż. Piotr Bąk

Otrzymują:

1. Wykonawcy, którzy pobrali/otrzymali SIWZ,
2. A/a.

Załącznik Nr 1 do pisma z dnia 27 kwietnia 2017 roku – dot. pyt. i odp. do SIWZ – Nr 1

Załacznik Nr 1 do SIWZ

FORMULARZ
OFERTY PRZETARGOWEJ

OFERTA DLA

Starostwo Powiatowe w Zakopanem
ul. Chramcówki 15
34-500 Zakopane

W postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego zgodnie z przepisami ustawy z dnia 29 stycznia 2004 roku – Prawo zamówień publicznych na: **„Wykonanie dostawy wraz z wdrożeniem urządzeń i oprogramowania zwiększających bezpieczeństwo sieci oraz infrastruktury serwerowej – część 1 dla potrzeb Starostwa Powiatowego w Zakopanem”**

1. DANE WYKONAWCY:

Osoba upoważniona do reprezentacji Wykonawcy/ów i podpisująca ofertę: ……..…..

……

Wykonawca/Wykonawcy:

Nazwa: ……..

……

……..

……..

Adres: ……

ul./nr: ……

kod/województwo: ……

NIP: ……

REGON: ……..……..

KRS/CEiDG: ……..……..……

Osoba odpowiedzialna za kontakty z Zamawiającym: ……

Dane teleadresowe na które należy przekazywać korespondencję związaną z niniejszym postępowaniem:

telefon: ……

faks: ……

e-mail: ……..……

www: ……

Adres do korespondencji (jeżeli inny niż adres siedziby): ……..

……..

……

2. OFEROWANY PRZEDMIOT ZAMÓWIENIA:

Oferuję wykonanie zamówienia pn. „Wykonanie adaptacji pomieszczeń pod centrum przetwarzania danych (serwerowania) w budynku Starostwa Powiatowego w Zakopanem” w szczegółowym zakresie objętym przedmiotem postępowania określonym w punkcie 3 przedmiotowej SIWZ do udziału w niniejszym postępowaniu.

Pakiet Nr 1
Infrastruktura zwiększająca bezpieczeństwo sieci oraz infrastruktura serwerowa

3.1. ŁĄCZNA CENA OFERTOWA BRUTTO PAKIETU NR 1:

Oferuję wykonanie zamówienia w zakresie objętym przedmiotem zamówienia określonym w SIWZ w zakresie Pakietu Nr 1 do udziału w niniejszym postępowaniu za ŁĄCZNĄ CENĘ OFERTOWĄ BTUTTO *:

ŁĄCZNA CENA OFERTOWA	**..... , ... zł brutto**

Powyższa łączna cena ofertowa zawiera doliczony zgodnie z obowiązującymi w Polsce przepisami podatek VAT, który na datę złożenia oferty **wynosi ..... %**.

* ŁĄCZNA CENA OFERTOWA BRUTTO stanowi całkowite maksymalne łączne wynagrodzenie należne wykonawcy w związku z realizacją przedmiotu niniejszego postępowania w zakresie Pakietu Nr 1 zgodnie z postanowieniami przedmiotowej SIWZ.

Oferuję dostawę następujących urządzeń spełniających wszystkie wymagania określone w OPZ do Pakietu Nr 1 (załącznik nr 6 do SIWZ) o następującej konstrukcji, parametrach technicznych, jakościowych i funkcjonalnych oraz ich przeznaczenia:

Modernizacja sieci LAN (przełączniki 10 Gbps i 1Gbps) – 1 kpl.

Producent / Firma:	**Podać: .....**
Urządzenie typ / model:	**Podać: .....**

Lp.	Parametr	Minimalne wymagania	Oferowany parametr
1.	Przeznaczenie	W ramach modernizacji sieci LAN należy wymienić przełączniki dystrybucyjne zastosowane w punktach dystrybucyjnych, łączące sieć strukturalną z zastosowaniem zabezpieczeń uwierzytelniania, tj.: - serwerownia główna: 1 szt. 24 x 1Gb/s, 1 szt. 24 x 1Gb/s z PoE - punkt dystrybucyjny: 2 szt. 48 x 1 Gb/s, 1 szt. 48 x 1 Gb/s z PoE - serwerownia backup: 2 szt. 48 x 1 Gb/s, 1 szt. 24 x 1 Gb/s z PoE	**TAK * / NIE ***
2.	Montaż	Urządzenie ma być zamontowane w szafie 19". Wysokość nie większa niż 1U wersja RACK. Montaż z użyciem dedykowanych uchwytów.	**TAK * / NIE ***
3.	Porty zainstalowane	Urządzenie powinno być wyposażone w następujące moduły: - Minimum 24 lub 48 porty GigabitEthernet w standardzie BaseT w zależności od wersji (24 x 1 Gb/s, 48 x 1Gb/s) - Wersja z PoE powinna obsługiwać przynajmniej połowę ilości portów przełącznika w standardzie PoE+ (tj. 12 /24 porty z PoE+) - minimum 4 porty 10Gb Ethernet w tym między innymi możliwość dedykowania dwóch portów 10Gb Ethernet SFP+ w celu połączenia przełączników w stos lub połączenia pomiędzy punktami dystrybucyjnymi - 1 port RJ45 umożliwiający zarządzanie poprzez konsolę	**TAK * / NIE ***
4.	Stos	Urządzenie powinno posiadać możliwość łączenia w stos minimum 4 przełączników tego samego typu z PoE lub bez. Urządzenia dostarczone przez Wykonawcę powinny być połączone wzajemnie w stos przynajmniej na poziomie punktu dystrybucyjnego.	**TAK * / NIE ***
5.	Wydajność	Urządzenie powinno posiadać następuje parametry minimalne: - Magistrala min.120 Gbps dla wersji 24 x 1 Gb/s lub min. 170 Gbps dla wersji 48 x 1 Gb/s - Prędkość przekazywanych pakietów: min. 95 Mpps dla wersji 24 x 1 Gb/s lub min. 130 Mbps dla wersji 48 x 1 Gb/s - Pamięć MAC adresów min. 16 000	**TAK * / NIE ***
6.	Obsługa	TACACS+, RADIUS, Link aggregation, Wsparcie dla agregacji LACP (802.3ad)	**TAK * / NIE ***
7.	Zarządzanie i bezpieczeństwo	Połączenie szyfrowane: SSL/SSH. Autentykacja dostępu do przełącznika w oparciu o Radius lub TACACS+. Listy dostępu (ACL) konfigurowalne dla fizycznego portu, łącza zagregowanego LAG i VLAN, Obsługa SNMP v2 i v3. Możliwość przechowywania dwóch wersji oprogramowania na przełączniku, 802.1x w tm: - MAC-based authentication, - MAC authentication bypass, - Guest VLAN Zarządzenie przez CLI i przez przeglądarkę internetową	**TAK * / NIE ***
		UWAGA – parametr służący wyłącznie ocenie ofert w kryterium wyboru oferty – Jakość Obsługa standardu mierzenia przepływu sieciowego np. sFlow,	**Jakość**: Obsługa standardu mierzenia przepływu

		NetFLow, IPFIX, : • Nie – 0 pkt, • Tak – 20 pkt.	sieciowego np. sFlow, NetFLow, IPFIX, : **TAK * / NIE ***
8.	Okablowanie	Wykonawca dostarczy komplet kabli połączeniowych w szczególności: kable statkujące - DAC, wkładki światłowodowe, krosowe światłowodowe oraz kable zasilające, itp.. Stackowanie przełączników jedynie przy użyciu kablami DAC lub światłowodowmi. Należy połączyć 3 punkty dystrybucyjne redundatnymi połączeniami SFP+ 10 Gb/s z przełącznikami rdzeniowymi w serwerowni głównej	**TAK * / NIE ***
9.	Zasilanie	1 zasilacz wbudowany	**TAK * / NIE ***
10.	Gwarancja	Gwarancja min. 5 lat. W ramach gwarancji naprawa lub wymiana sprzętu na nowy. Czas reakcji serwisu w następnym dniu roboczym. Gwarancja obejmująca przełącznik oraz moduły i kable. W ramach gwarancji dostęp do nowych wersji oprogramowania.	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Gwarancja Wydłużenie okresu gwarancji przez okres posiadania sprzętu: • Gwarancja: 60 miesięcy – 0 pkt, • Gwarancja: dożywotnia – 15 pkt.	**Gwarancja** (Podać): **…… m-cy**
11.	Certyfikaty	przełącznik musi posiadać deklaracja CE, został wyprodukowany zgodnie z normą ISO-9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność	**TAK * / NIE ***
12.	Stan	Fabrycznie nowy	**TAK * / NIE ***

* **Niepotrzebne skreślić**

Przełącznik rdzeniowy (switch) 10G – 2 szt.

Producent / Firma:	**Podać: ……**
Urządzenie typ / model:	**Podać: ……**

Lp.	Parametr	Minimalne wymagania	Oferowany parametr
1.	Przeznaczenie:	Przełącznik zastosowany jako rdzeniowy łączący połączenia serwerów, macierzy oraz przełączników dystrybucyjnych.	**TAK * / NIE ***
2.	Montaż:	Urządzenie musi mieć możliwość montażu w szafie 19”. Wysokość nie większa niż 1U wersja RACK. Montaż z użyciem dedykowanych uchwytów.	**TAK * / NIE ***
3.	Porty zainstalowane:	Urządzenie powinno umożliwiać instalację następujących modułów: min. 24 x 10 GbE SFP+ w tym moduł min. 2 porty 40GbE QSFP+ umożliwiające zestackowanie przełączników.	**TAK * / NIE ***
4.	Stos:	Urządzenie powinno zapewniać łączenie w stos minimum 4 przełączników. Urządzenia dostarczone przez Wykonawcę powinny być połączone wzajemnie w stos portami 40Gbe.	**TAK * / NIE ***
5.	Wydajność:	Urządzenie powinno posiadać następuje parametry minimalne: Magistrala min. 600 Gbps; Prędkość przekazywanych pakietów: min. 450 Mpps. Pamięć MAC adresów min. 130 000	**TAK * / NIE ***
6.	Obsługa:	Przełącznik warstwy 3 TACACS+, RADIUS, , Link aggregation, Wsparcie dla agregacji LACP (802.3ad)	**TAK * / NIE ***
7.	Zarządzanie i bezpieczeństwo	Połączenie szyfrowane: SSL/SSH, Autentykacja dostępu do przełącznika w oparciu o Radius lub TACACS+ Listy dostępu (ACL) konfigurowalne dla fizycznego portu, łącza zagregowanego LAG i VLAN, Obsługa SNMP v2 i v3, Obsługa sFlow, Możliwość przechowywania dwóch wersji oprogramowania na przełączniku, 802.1x w tm: - MAC-based authentication, - MAC authentication bypass, - Guest VLAN Zarządzenie przez CLI i przez przeglądarkę internetową, Port mirroring Liczniki pakietów wchodzących/wychodzących per każdy port Broadcast storm control	**TAK * / NIE ***
8.	Okablowanie :	Wykonawca dostarczy kable przyłączeniowe do połączenia oferowanego urządzenia z dostarczanymi urządzeniami sieciowymi w szczególności: kable do statkowania kable krosowe światłowodowe wkładki światłowodowe oraz kable zasilające. Dodatkowo przełącznik powinien zapewniać podłączenie serwerów, np. powinien mieć	**TAK * / NIE ***

		zainstalowane przynajmniej wkładki 4 szt. 1 GbE T/przełącznik oraz 4 szt. 10 GbE SFP+ (dopuszcza się rozwiązanie połączenia za pomocą kabli DAC/TWINAX)/przełącznik,	
9.	Obudowa:	2 zasilacze redundantne wbudowane, redundantne wiatraki, chłodzenie przełącznika od portów Eth w kierunku zasilaczy (od przodu do tyłu urządzenia ze względu na strefy ciepła/zimna)	**TAK * / NIE ***
10.	Gwarancja:	Min. 5 lat gwarancji obejmująca przełącznik oraz moduły i kable. W ramach gwarancji dostęp do nowych wersji oprogramowania. W ramach gwarancji naprawa lub wymiana sprzętu na nowy. Czas reakcji serwisu w następnym dniu roboczym.	**TAK * / NIE ***
11.	Certyfikaty:	przełącznik musi posiadać deklaracja CE, został wyprodukowany zgodnie z normą ISO-9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność	**TAK * / NIE ***
12.	Stan	Fabrycznie nowy	**TAK * / NIE ***

* **Niepotrzebne skreślić**

Modernizacja sieci WiFi (centralnie zarządzalne punkty WiFi) – 1 kpl.

Producent / Firma:	**Podać: ……**
Urządzenie typ / model:	**Podać: ……**

Lp.	Parametr	Minimalne wymagania	Oferowany parametr
1.	Przeznaczenie	Modernizacja obecnie użytkowanych punktów dostępowych oraz dołożenie nowych w wymaganych do pokrycia zasięgiem sygnału WiFi obszaru na którym będą użytkowane urządzenia mobilne.	**TAK * / NIE ***
2.	Montaż	8 sztuk punktów WiFi należy zamontować we wskazanych miejscach przez Zamawiającego do sufitu pomieszczeń budynku. Należy doprowadzić okablowanie z punktów dystrybucyjnych do niniejszych punktów WiFi.	**TAK * / NIE ***
3.	Kontroler	Urządzenia zarządzane i zintegrowane na poziomie dostarczanego UTM. Zarządzanie z GUI wspólnego z UTM.	**TAK * / NIE ***
4.	Prędkość	Maksymalna powyżej 1 Gbps	**TAK * / NIE ***
5.	Parametry fizyczne	1 x 1000BASE-T IEEE 802.3af/at Obsługa technologii 802.11n i praca w technice transmisji wieloantenowej MIMO 3x3	**TAK * / NIE ***
6.	Wspierane protokoły i funkcje	802.11a/b/g/n/ac, 802.11i, 802.1q, 802.1X, 802.3af/at, 802.11e, 2.4 oraz 5 GHz	**TAK * / NIE ***
7.	Dodatkowe:	Wraz z punktem dostępowym należy dostarczyć dedykowany uchwyt umożliwiający montaż punktu dostępowego pod sufitem.	**TAK * / NIE ***
8.	Gwarancja:	Min. 3 lata gwarancji. W ramach gwarancji dostęp do nowych wersji oprogramowania. W ramach gwarancji naprawa lub wymiana sprzętu na nowy. Czas reakcji serwisu w ciągu 3 dni roboczych.	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Gwarancja Wydłużenie okresu gwarancji: • Gwarancja: 36 miesięcy – 0 pkt, • Gwarancja: 37 – 44 miesięcy – 1 pkt, • Gwarancja: 45 – 50 miesięcy – 2 pkt, • Gwarancja: 51 – 55 miesięcy – 3 pkt, • Gwarancja: 56 – 59 miesięcy – 4 pkt, • Gwarancja: 60 miesięcy – 5 pkt,	**Gwarancja** (Podać): **…… m-cy**
9.	Certyfikaty:	Urządzenie musi posiadać certyfikat CE, został wyprodukowany zgodnie z normą ISO-9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność	**TAK * / NIE ***
10.	Stan	Fabrycznie nowy	**TAK * / NIE ***

* **Niepotrzebne skreślić**

Zakup zestawu UTM (klaster) - ochrona styku Internet/Intranet

Producent / Firma:	**Podać: ……**

Urządzenie typ / model:		Podać: ……	
Lp.	**Parametr**	**Minimalne wymagania**	**Oferowany parametr**
1.	Architektura	System musi być dostarczony w postaci dwóch fizycznych urządzeń (obydwa urządzenia muszą by tego samego modelu). Do urządzeń musi być dostarczony niezbędny zestaw wyposażenia technicznego w tym np. kable, oraz licencje pozwalające na pracę dwóch urządzeń w trybie klastra HA (High Availability) typu active/active lub active/passive	**TAK * / NIE ***
2.	Funkcjonalności rozwiązania	Musi wspierać trzy strefy bezpieczeństwa (DMZ) Musi wspiera statyczne i dynamiczne adresy IP (DHCP i PPoE) na zewnętrznym interfejsie. Przepustowość Firewall: Musi obsługiwać przepustowość UTM min. 500 Mbps Musi obsługiwać min. 1 700 000 jednoczesnych połączeń Urządzenie musi posiadać cechy zabezpieczenia UTM, włącznie z filtrowaniem zawartości URL, IPS, GAV, kontroli aplikacji, DLP, oraz ochroną przed zagrożeniami typu zero-day Musi posiadać wsparcie dla implementacji polityki bezpieczeństwa w warstwie aplikacji jako proxy aplikacji. Rozwiązanie musi zawierać zasady bezpieczeństwa proxy w warstwie aplikacji, skonfigurowane domyślnie do wspierania następujących wspólnych protokołów: HTTP, HTTPs, POP3, SMTP, FTP, DNS, SIP, H323 Urządzenie musi wspierać uwierzytelnianie poprzez RADIUS, SecureID, LDAP i Active Directory. Musi obsługiwać uwierzytelnianie serwerów Active Directory w trybie transparent (Single-Sign-On). W urządzeniu nie powinno być żadnych ograniczeń liczby użytkowników pracujących online. Musi posiadać wsparcie Dynamic DNS. Rozwiązanie musi posiadać obronę przeciwko pofragmentowanym atakom, dzięki czemu będzie w stanie zmontować pofragmentowane pakiety przed przekazaniem ich do sieci wewnętrznej. Urządzenie musi mieć funkcjonalność pozwalającą na filtrowanie treści najpopularniejszych protokołów, jak i również na filtrowanie według typu MIME. Musi mieć możliwość chronienia wewnętrznych serwerów pocztowych przeciwko atakom typu spam z możliwością konfiguracji komputera dla domen akceptujących e-mail. Musi posiadać możliwość konfiguracji progów bezpieczeństwa dla wykrywania ataków typu flood, DoS, oraz DDoS Firewall musi wspierać protokół wykrywania anomalii w DNS i w innych popularnych protokołach.	**TAK * / NIE ***
3.	VPN	Musi posiadać wsparcie dla mobilnych sieci VPN Musi obsługiwać co najmniej 20 mobilnych połączeń VPN IPSec Musi obsługiwać co najmniej 20 mobilnych połączeń VPN SSL Musi posiadać możliwość pobrania klienta SSL bezpośrednio z urządzenia Niezbędna jest dostępność klienta SSL dla przynajmniej dla systemów operacyjnych posiadanych przez Zamawiającego: Windows Vista, Windows 7, 8, 10 jak i również dla Android Musi posiadać wsparcie dla VPN pomiędzy oddziałami Musi obsługiwać co najmniej 5 połączeń VPN między oddziałami poprzez IPSec Urządzenie musi być w stanie współdziałać z produktami innych marek, które wspierają obsługę IPSec Rozwiązanie musi wspierać mechanizmy uwierzytelniania DES, 3DES, AES 128 -, 192 -, 256-bit Rozwiązanie musi wspierać mechanizmy szyfrowania SHA-1, SHA-2,MD5, IKE Pre-Shared Key, 3rd Party Cert. Musi posiadać wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego) Musi posiadać przepustowość IPSec VPN nie mniejsza niż 1200 Mbps Musi mieć możliwość tworzenia wirtualnych interfejsów VPN site-site oraz VPN poprzez Dynamic Routing Protocols	**TAK * / NIE ***
4.	Filtrowanie zawartości URL i kontrola aplikacji	Możliwość wspierania filtrowania zawartości w urządzeniu poprzez stosowanie subskrypcji Funkcjonalność filtrowania zawartości powinna zawierać możliwość filtrowania użytkowników lub grup użytkowników Rozwiązanie powinno pozwalać na tworzenie białych list wyjątków dla filtrowania zawartości Baza zawartości URL powinna być dynamicznie aktualizowana Funkcja powinna filtrować treści w wielu językach, w tym w języku polskim Urządzenie powinno identyfikować i blokować wiele różnych aplikacji, w tym mieć możliwość szczegółowej kontroli funkcji i aplikacji, takich jak logowanie i transfer plików. Niezbędna jest automatyczna i regularna aktualizacja sygnatur aplikacji	**TAK * / NIE ***

5.	Antywirus	Musi posiadać możliwość wsparcia systemu antywirusowego z poziomu urządzenia poprzez subskrypcje Musi posiadać automatyczną aktualizację plików sygnatur antywirusowych Antywirus musi mieć możliwość przeprowadzania kwarantanny e-mail. Rozwiązanie musi mieć możliwość tworzenia wyjątków w białej liście, aby umożliwić nieblokowany dostęp do poczty z określonych domen Musi posiadać blokowanie spyware Musi posiadać skanowanie wszystkich plików skompresowanych (np.: zip, tar, rar, gzip) z wieloma poziomami kompresji Musi posiadać wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3 Musi posiadać możliwość funkcjonalności opartej na chmurze pozwalającej na wprowadzenie oceny reputacji Usługa musi być w stanie zablokować strony internetowe ze złą reputacją bazując na informacjach pobranych z chmury (historia wirusów, smapu i innych rodzajów złośliwego oprogramowania) Musi posiadać przepustowość AV w urządzeniu nie mniejsza niż 600 Mbps	**TAK * / NIE ***
6.	Antyspam	Możliwość wsparcia systemu antyspamowego z poziomu urządzenia poprzez subskrypcje Antyspam musi zapewnić możliwość kwarantanny e-mail Antyspam musi posiadać zintegrowaną antywirusową analizę spamu Rozwiązanie musi umożliwić blokowanie spamu w wielu językach w tym w języku polskim Musi posiadać możliwość blokowania spamu opartego na obrazach graficznych (OCR).	**TAK * / NIE ***
7.	IPS	Musi posiadać możliwość wsparcia IPS z poziomu urządzenia poprzez subskrypcje Musi posiadać automatyczną aktualizacja sygnatur IPS IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy Musi posiadać automatyczne blokowanie znanych źródeł ataków Musi posiadać wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3 Musi posiadać przepustowość IPS w urządzeniu nie mniejszą niż 1 Gbps	**TAK * / NIE ***
8.	NAT	Urządzenie musi wpierać NAT i PAT. Musi posiadać wspieranie równoważenia obciążenia serwerów dla urządzeń wewnętrznych Musi posiadać wsparcie dla Static NAT (Port Forwarding) Musi posiadać wsparcie dla Dynamic NAT Musi posiadać wsparcie dla NAT One-to-One Musi posiadać wsparcie dla IPSec NAT Traversal Musi posiadać wsparcie dla policy-based NAT	**TAK * / NIE ***
9.	Parametry sieciowe	Ilość interfejsów sieciowych: minimum 8x 10/100/1000 BaseT interface. Interfejsy te powinny być skonfigurowane jako jeden z trzech rodzajów wymaganych stref bezpieczeństwa Wsparcie Multi-WAN. Urządzenie musi obsługiwać co najmniej trzy zewnętrzne źródła połączenia z Internetem. Interfejsy te muszą umożliwiać działanie w trybie fail-over Interfejsy zewnętrzne muszą również działać w trybie „round-robin” Interfejsy zewnętrzne muszą również działać jako „overflow" Wsparcie VLAN: musi posiadać minimum 10 sieci VLAN Urządzenie musi także zapewniać kontrolę ruchu dla użytkowników, polityk, protokołu, grupy użytkowników. Musi zapewnić kontrolę ruchu dla wszystkich interfejsów. Musi zapewnić kontrolę ruchu adresu IP oraz sieci VLAN Musi zapewnić kontrolę ruchu aplikacji i kategorii aplikacji Rozwiązanie musi wspierać implementację w trybie routera (routing), tryb drop-in (ten sam adres IP na wszystkich interfejsach), oraz w trybie transparent-bridge Powinno musi wspierać statyczny i dynamiczny NAT, oraz 1-1 NAT Rozwiązanie musi pracować w trybie HA Musi posiadać wsparcie dla routingu opartego na regułach (Policy Based Routing)	**TAK * / NIE ***
10.	Zarządzenie	Administracja urządzenia musi być możliwe poprzez graficzny interfejs zarządzania w czasie rzeczywistym. Musi zapewniać monitorowanie logów ruchu w czasie rzeczywistym. Rozwiązanie musi zapewniać wysyłanie alarmów przez SNMP lub e-mail. Musi posiadać wsparcie zarządzania protokołami DVCP (Dynamic VPN Control Protocol). Musi posiadać obsługę różnych ról administratorów. Użytkownicy muszą być uwierzytelnieni przez zewnętrzny serwer z użytkownikami.	**TAK * / NIE ***

		Urządzenie musi wspierać zarządzanie przez przeglądarkę WWW. Urządzenie musi zapewniać zarządzanie za pomocą linii poleceń poprzez port szeregowy lub poprzez SSH. Interfejs WWW do zarządzania urządzeniem musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach mobilnych typu tablet lub smartfon. System musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia, bez konieczności podłączenia się do niego.	
11.	Dzienniki i raporty	Oferowane rozwiązanie musi umożliwić stosowanie serwerów zewnętrznych w drodze do scentralizowania przechowywania dzienników i raportów. Niedopuszczalne jest stosowanie dodatkowych opłat za rozwiązanie do rejestrowania i raportowania Usługa musi być oparta na TCP oraz korzystać z bazy danych SQL, aby zapewnić jej pełną skalowalność. Powinno być możliwe zdefiniowanie wielu serwerów dziennika. Urządzenie musi mieć możliwość współpracy z dwoma serwerami dzienników, jednego głównego, oraz drugiego w przypadku awarii. Dzienniki transmisji muszą być odpowiednio szyfrowane. Rozwiązanie musi posiadać ponad 50 predefiniowanych typów raportów, bez żadnych dodatkowych opłat i kosztów. Urządzenie musi mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV. System musi być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania tych sprawozdań pocztą e-mail. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości. System raportowania powinien być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów i dzienników. Narzędzie do tworzenia dzienników i raportów musi wspierać posiadaną przez Zamawiającego platformę Vmware. System musi zapewniać wizualizację, opisującą w trybie graficznym stan przepustowości systemu. System musi mieć możliwość przedstawienia na mapie świata źródła i celów zagrożeń, ruchu aplikacji, blokowania dostępu oraz wydarzeń IPS. Raporty IPS muszą prowadzić do portalu internetowego dostarczającego szczegółowe informacje dotyczącego każdego zdarzenia. Możliwość grupowania urządzeń, w celu tworzenia raportów sumarycznych.	**TAK * / NIE ***
12.	Blokowanie APT	Musi posiadać możliwość wsparcia blokowania dla nieznanego złośliwego oprogramowania z poziomu urządzenia poprzez subskrypcje	**TAK * / NIE ***
13.	Oprogramowanie monitorujące (sensory)	Musi posiadać w zestawie możliwość instalacji sensorów na stacjach klienckich w celu wykrywania stanu bezpieczeństwa stacji. Wymagana dostawa subskrypcji	**TAK * / NIE ***
14.	Gwarancja	Urządzenia muszą być dostarczone z min. 3 letnią gwarancja, świadczoną w następnym dniu roboczym, oraz z bezpłatną subskrypcją aktualizacji oprogramowania oraz definicji sygnatur w okresie obowiązywania gwarancji.	**TAK * / NIE ***
15.	Certyfikaty:	Urządzenie musi posiadać certyfikat CE, został wyprodukowany zgodnie z normą ISO-9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność	**TAK * / NIE ***
16.	Stan	Fabrycznie nowy	**TAK * / NIE ***

*** Niepotrzebne skreślić**

Oświadczam(y), że oferowany powyżej urządzenia posiadają i spełniają wszystkie wymagane minimalne warunki dotyczące ich konstrukcji, parametrów technicznych, jakościowych i funkcjonalnych oraz ich przeznaczenia określone w OPZ stanowiącym załacznik nr 6 do przedmiotowej Specyfikacji Istotnych Warunków Zamówienia oraz są kompletne i gotowy do użytkowania bez konieczności ponoszenia przez zamawiającego żadnych dodatkowych kosztów.

Pakiet Nr 2
Oprogramowanie zwiększające bezpieczeństwo sieci

3.2. ŁĄCZNA CENA OFERTOWA BRUTTO PAKIETU NR 2:

Oferuję wykonanie zamówienia w zakresie objętym przedmiotem zamówienia określonym w SIWZ w zakresie Pakietu Nr 2 do udziału w niniejszym postępowaniu za ŁĄCZNĄ CENĘ OFERTOWĄ BTUTTO *:

ŁĄCZNA CENA OFERTOWA	

	..... , ... zł brutto

Powyższa łączna cena ofertowa zawiera doliczony zgodnie z obowiązującymi w Polsce przepisami podatek VAT, który na datę złożenia oferty **wynosi ..... %**.

* ŁĄCZNA CENA OFERTOWA BRUTTO stanowi całkowite maksymalne łączne wynagrodzenie należne wykonawcy w związku z realizacją przedmiotu niniejszego postępowania w zakresie Pakietu Nr 2 zgodnie z postanowieniami przedmiotowej SIWZ.

Oferuję dostawę następujących urządzeń spełniających wszystkie wymagania określone w OPZ do Pakietu Nr 2 (załącznik nr 7 do SIWZ) o następującej konstrukcji, parametrach technicznych, jakościowych i funkcjonalnych oraz ich przeznaczenia:

Pakiet oprogramowania monitorowania bezpieczeństwa IT			
Producent / Firma:		**Podać: .....**	
Urządzenie typ / model:		**Podać: .....**	
Lp.	**Parametr**	**Minimalne wymagania**	**Oferowany parametr**
1.	Przeznaczenie	Pakiet oprogramowania monitorowania bezpieczeństwa IT będzie dotyczył bezpieczeństwa teleinformatycznego w dwóch głównych obszarach: - monitorowanie sieci oraz zarządzanie zdarzeniami i logami - monitorowanie i zarządzaniem sprzętem komputerowym oraz użytkownikami W związku ze stale rosnącymi zagrożeniami wymaga się dostawy pakietu oprogramowania monitorowania IT obejmujący funkcjonalności niezbędne do podniesienia bezpieczeństwa teleinformatycznego: wykrywanie i skanowanie sieci, stałe monitorowanie zagrożeń, zbieranie i zarządzanie logami oraz korelacja zdarzeń, audyt zasobów sprzętowych i oprogramowania, monitorowanie aktywności użytkowników, pomoc użytkownikom sieci, kontrola dostępu użytkowników do urządzeń i nośników danych oraz alarmowanie i raportowanie	**TAK * / NIE ***
2.	Licencja	Licencja na pakiet oprogramowania jest bezterminowa. Musi zostać zapewnione minimum 1 roczny okres aktualizacji oprogramowania, subskrypcji oraz wsparcie producenta. Pakiet oprogramowania powinien zapewniać dostęp do konsoli zarządczej przynajmniej trzem administratorom. Dopuszcza się zaoferowanie dwóch licencji programów w pakiecie (ze względu na nieograniczanie konkurencji) obsługujących poszczególne obszary bezpieczeństwa pakietu oprogramowania.	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Subskrypcja Wydłużenie okresu aktualizacji oprogramowania, subskrypcji zagrożeń dotyczących obszaru monitorowania sieci oraz zarządzania zdarzeniami i logami: • Subskrypcja: 12 miesięcy – 0 pkt, • Subskrypcja: 13 – 15 miesięcy – 5 pkt. • Subskrypcja: 16 – 18 miesięcy – 10 pkt. • Subskrypcja: 19 – 21 miesięcy – 15 pkt. • Subskrypcja: 22 – 23 miesięcy – 20 pkt. • Subskrypcja: 24 miesiące – 30 pkt.	**Subskrypcja** (Podać): **..... m-cy**
3.	Monitorowanie sieci oraz zarządzanie zdarzeniami i logami	Rozwiązanie musi umożliwiać wdrożenie pełnej wymaganej funkcjonalności na platformie wirtualizacyjnej. Rozwiązanie musi być zdolne do identyfikacji ruchu sieciowego w sieciach środowisk wirtualnych. System musi zapewniać możliwość zbierania logów z co najmniej 25 źródeł Rozwiązanie powinno posiadać wsparcie producenta, ale też wsparcie w formie dostępnego forum wymiany wiedzy/doświadczeń dotyczące produktu, które zostanie udostępnione bez limitu operatorom i administratorom systemu. Rozwiązanie musi wspierać długoterminowe zapewnienie dostępu do	**TAK * / NIE ***

		szczegółowych danych odnośnie zarejestrowanych i zebranych zdarzeń czy przepływów w sieci. System powinien zapewnić dostęp do takich informacje co najmniej przez okres trwania subskrypcji. Licencja powinny być bezterminowe i nie uzależnione od wykupienia lub przedłużenia wsparcia producenta.	
		W zakresie monitorowania sieci oraz zarządzanie zdarzeniami i logami musi zapewnić: Wykrywanie i skanowanie sieci, Stałe monitorowanie zagrożeń, Zbieranie i zarządzanie logami, Korelacja zdarzeń	**TAK * / NIE ***
		Rozwiązanie musi zapewnić możliwość uchwycenia i prezentacji wszystkich istotnych aspektów incydentu bezpieczeństwa w jednym logicznym widoku. Widok taki powinien zawierać minimalnie informacje typu: powiązane zdarzenia, aktywność sieciowa, skorelowane alerty, skorelowane podatności w powiązanych systemach, itp.	**TAK * / NIE ***
		Rozwiązanie musi umożliwiać szyfrowanie komunikacji pomiędzy poszczególnymi modułami systemu i zbierania danych. Rozwiązanie musi umożliwiać integrację z zewnętrznymi dostawcami mechanizmów uwierzytelniania (LDAP, AD, RADIUS, etc...) dla operatorów i administratorów systemu	**TAK * / NIE ***
		Rozwiązanie musi wspierać informacje NetFlow - czyli dane o przepływach, np.: NetFlow, J- Flow, sFlow, IPFIX, itp.	**TAK * / NIE ***
		Wykrywanie i rejestrowanie dla celów audytowych zmian w konfiguracji urządzeń sieciowych, zawiadamianie użytkowników o działaniu niezgodnym ze zdefiniowanymi politykami (zasadami). Możliwość analizy na poziomie sieciowym, kto był zaangażowany w incydent, co się stało, kiedy zaszło zdarzenie, jakie dane zostały udostępnione lub przekazane.	**TAK * / NIE ***
		Rozwiązanie musi posiadać mechanizmy usprawniające jego wykorzystanie i wdrożenie, np.: - automatyczne wykrywanie źródeł logów - automatyczne wykrywanie aplikacji - automatyczne wykrywanie aktywów - automatyczne wykrywanie podatności - automatyczne wykrywanie anomalii - automatyczne grupowanie aktywów - predefiniowane reguły analizy i korelacji zdarzeń - łatwe w użyciu mechanizmy filtrowania (również predefiniowane filtry) - zaawansowane funkcje analizy zabezpieczeń - predefiniowane raporty - priorytetyzacja wg zasobów - automatyczne aktualizacje baz zagrożeń, wsparcia urządzeń, oprogramowania systemowego,	**TAK * / NIE ***
		Rozwiązanie musi zapewniać ciągłe działanie jak największej liczby komponentów, niezależnie od awarii jednego z nich. Np. w sytuacji awarii systemu centralnego lub modułu analitycznego, logi powinny być nadal zbierane. Rozwiązanie musi posiadać mechanizmy umożliwiające zbieranie danych w czasie rzeczywistym.	**TAK * / NIE ***
		Rozwiązanie powinno posiadać pewną ilość przykładowych skonfigurowanych paneli (dashboards), prezentujących możliwości i mechanizmy systemu.	**TAK * / NIE ***
		Rozwiązanie musi utrzymywać bazę wiedzy o wszystkich wykrytych w sieci aktywach. Wśród zgromadzonych danych o danym aktywie powinny być zawarte pewne informacje uzyskane przy wykrywaniu zasobów: - atrybuty systemu - atrybuty sieciowe - stan - podatności/luki - lokalizacja - przynależność - inne właściwości, które użytkownik może samodzielnie zdefiniować i/lub wpisywać.	**TAK * / NIE ***
		Rozwiązanie musi wspierać informacje zbierane z systemów operacyjnych w wersji serwerowej. Rozwiązanie musi wspierać informacje zebrane z infrastruktury sieciowej (switche, routery, itp.). Rozwiązanie musi posiadać własny skaner podatności.	**TAK * / NIE ***
		Rozwiązanie musi zapewniać możliwość przechowywania zarówno znormalizowanych danych o zdarzeniach, jak również	**TAK * / NIE ***

		źródłowego/oryginalnego formatu danych w tzw. postaci RAW, np. dla celów późniejszej analizy w innych systemach lub przeprowadzenia analizy śledczej.	
		Rozwiązanie musi posiadać architekturę pozwalającą na zbieranie i archiwizację logów, w podziale na dane krótkoterminowe (tzw. online, wykorzystywane w bieżących analizach) oraz dane długoterminowe (tzw. offline, dane archiwizowane po określonym czasie), z wewnętrzną ale konfigurowalną obsługą mechanizmu retencji danych pomiędzy obydwoma typami. Rozwiązanie powinno wspierać przechowywanie (archiwizację) logów na zewnętrznych urządzeniach do składowania danych. Rozwiązanie musi wspierać mechanizmy zbierania logów (np.: syslog, WMI, JDBC, SNMP, itp.). System powinien wspierać analizę logów z systemów operacyjnych posiadanych przez Zamawiającego, tj. Windows Serwer, Linux	**TAK * / NIE ***
		Rozwiązanie musi zapewniać raportowanie dla wszystkich przedmiotów dostępnych poprzez GUI systemu (np.: pobrane dane, zanalizowane dane, zdarzenia, przepływy, podatności, zasoby, zagrożenia, itp.). Rozwiązanie musi posiadać konfigurowalny silnik raportowania, tak aby możliwe było tworzenie niestandardowych raportów bez dodatkowych kosztów (licencje i wsparcie techniczne) usług ze strony producenta. Rozwiązanie musi zapewnić szablony do szybkiego tworzenia i dostarczania raportów na wielu poziomach szczegółowości.	**TAK * / NIE ***
		Rozwiązanie musi realizować analizę i sygnalizowanie incydentów nie tylko na zasadzie przekroczenia ustalonego progu dla zdarzeń, ale również na zasadzie analizy behawioralnej i oceny anomalii w trendzie. Rozwiązanie musi generować alerty na podstawie zauważonej zmiany w sieci dotyczącej pojawienia się nowej usługi lub gdy pojawią się nowe zasoby,	**TAK * / NIE ***
		Rozwiązanie musi posiadać zdolność korelowania zdarzeń z informacjami pozyskanymi ze znanych skanerów luk bezpieczeństwa	**TAK * / NIE ***
		Rozwiązanie musi wspierać różne standardy komunikacji, w celu przekazywania alertów do innych rozwiązań.	**TAK * / NIE ***
4.	Monitorowanie i zarządzaniem sprzętem komputerowym oraz użytkownikami	Rozwiązanie musi umożliwiać wdrożenie pełnej wymaganej funkcjonalności na platformie wirtualizacyjnej. Dopuszcza się możliwość wykonania dostawy oprogramowania zbiorczego na urząd będź dostarczone oprogramowanie musi obsługiwac przynajmniej 130 urządzeń (unikalnych adresów IP) w celu należytego monitorowania bezpieczeństwa urządzeń w sieci urzędu. Rozwiązanie w niniejszym zakresie musi udostępniać funkcjonalności: Audyt zasobów sprzętowych i oprogramowania: - Lista aplikacji oraz aktualizacji systemu operacyjnego na pojedynczej stacji roboczej (rejestr) - Lista aplikacji oraz aktualizacji systemu operacyjnego na pojedynczej stacji roboczej (skan dysków) - Numery seryjne (klucze) oprogramowania - Informacje o plikach wykonywalnych i wpisach rejestrowych na stacji roboczej - Informacje o plikach multimedialnych (mp3, avi itp.) oraz archiwach zip i ich metadanych (tytuł i autor utworu, zawartość pliku zip) - Ogólne informacje o sprzęcie stacji roboczej - Szczegółowe informacje o sprzęcie stacji roboczej (model, płyta, procesor, pamięć, napędy, karty itp.) - Informacje systemowe (komendy startowe, konta użytkowników, foldery udostępnione, informacje SMART itp.) - Audyt inwentaryzacji sprzętu i oprogramowania - Baza wzorców oprogramowania - Zarządzanie licencjami - Historia zmian sprzętu i oprogramowania - Środki Trwałe: baza ewidencji majątku IT (definiowanie własnych typów środków, ich atrybutów oraz wartości, załączniki, import danych z pliku CSV) - Alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych - Skaner inwentaryzacji offline - Skanowanie i drukowanie kodów kreskowych oraz QR	**TAK * / NIE ***

		Monitorowanie aktywności użytkowników: - Ogólne informacje o aktywności użytkownika - Szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy) - Użytkowane aplikacje (aktywnie i nieaktywnie, czyli całkowity czas działania aplikacji oraz czas faktycznego używania jej przez użytkownika) - Blokowanie uruchamianych aplikacji - Odwiedzane strony WWW (tytuły i adresy stron, ilość i czas wizyt) - Blokowanie stron WWW - Wydruki: audyt (per: drukarka, użytkownik, komputer), koszty wydruków - Wysłane i odebrane wiadomości e-mail (nagłówki) - Użycie łącza: generowany przez użytkowników ruch sieciowy (wchodzący i wychodzący, lokalny i internetowy) - Statyczny zdalny podgląd pulpitu użytkownika (bez dostępu) - Zrzuty ekranowe (historia pracy użytkownika "ekran po ekranie")	**TAK * / NIE ***
		Pomoc użytkownikom sieci: - Baza zgłoszeń serwisowych - Tworzenie zgłoszeń i zarządzanie zgłoszeniami (przypisywanie do administratorów z powiadamianiem e-mail) - Komentarze i załączniki w zgłoszeniach - Zrzuty ekranowe w zgłoszeniach - Wewnętrzny komunikator (czat) - Komunikaty wysyłane do użytkowników/komputerów z możliwym obowiązkowym potwierdzeniem odczytu - Statyczny zdalny podgląd pulpitu użytkownika (bez dostępu) - Zdalny dostęp do komputerów (pracownik, jak i administrator widzą ten sam ekran) z możliwym pytaniem użytkownika o zgodę - Zadania dystrybucji oraz uruchamiania plików (jeśli komputer jest wyłączony podczas uruchamiania dystrybucji, dojdzie ona do skutku po jego uruchomieniu) - Integracja bazy użytkowników z AD - Przypisywanie pracowników helpdesk do kategorii zgłoszeń - Procesowanie zgłoszeń z wiadomości e-mail - Baza wiedzy	**TAK * / NIE ***
		Kontrola dostępu użytkowników do urządzeń i nośników danych - Urządzenia podłączone do danego komputera - Lista wszystkich urządzeń podłączonych do komputerów w sieci - Audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych - Zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników (np. autoryzowanie firmowych szyfrowanych pendrive'ów, a blokowanie pendrive'ów prywatnych pracowników) - Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników AD - Integracja bazy użytkowników i grup z AD - Alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym	**TAK * / NIE ***
		Alarmowanie i raporty: - Alarmy zdarzenie-akcja (np. gdy ważne parametry znajdą się poza zakresem zdefiniowanym przez użytkownika) - Powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.) - Raporty (dla użytkownika, urządzenia, oddziału, mapy sieci lub całego atlasu)	**TAK * / NIE ***

* **Niepotrzebne skreślić**

Pakiet oprogramowania antywirusowego	
Producent / Firma:	**Podać: ……**
Urządzenie typ / model:	**Podać: ……**

Lp.	Parametr	Minimalne wymagania	Oferowany parametr
1.	Przeznaczenie	Pakiet oprogramowania antywirusowego będzie stanowił element zwiększających bezpieczeństwo sieciowe w organizacji, tj. Wydziału Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami oraz serwerów na których będą uruchomione usługi przed złośliwym oprogramowaniem	**TAK * / NIE ***
2.	Licencja	W ramach dostawy pakietu oprogramowania antywirusowego Zamawiający musi zostać wyposażony w: - zestaw oprogramowania wraz z licencjami umożliwiającymi scentralizowaną ochronę antywirusową sieci składającej się z 35 komputerów oraz serwerów, - dokumentację w postaci elektronicznej - w języku polskim, - Zamawiający wymaga, by dostarczone oprogramowanie było objęte 1 roczną opieką aktualizacyjną w zakresie udostępniania przez producenta nowych wersji oprogramowania oraz aktualizacji sygnatur.	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Subskrypcja Wydłużenie okresu opieki aktualizacyjnej w zakresie udostępniania przez producenta nowych wersji oprogramowania oraz aktualizacji sygnatur: • Subskrypcja: 12 miesięcy – 0 pkt, • Subskrypcja: 13 – 18 miesięcy – 2 pkt. • Subskrypcja: 19 – 24 miesięcy – 4 pkt. • Subskrypcja: 25 – 30 miesięcy – 6 pkt. • Subskrypcja: 31 – 35 miesięcy – 8 pkt. • Subskrypcja: 36 miesiące – 10 pkt.	**Subskrypcja** (Podać): **..... m-cy**
3.	Ogólne właściwości oprogramowania antywirusowego	- Oprogramowanie antywirusowe musi być dostępne w pakietach instalacyjnych dla stacji roboczych oraz serwerów. Dostarczane klucze licencyjne muszą pozwalać na aktywowanie oprogramowania przeznaczonego do ochrony stacji roboczych oraz serwerów. - Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami, ransomware i innymi potencjalnie niebezpiecznymi programami. - Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony. - Program ma mieć możliwość skanowania i klasyfikowania plików oraz odsyłaczy do zasobów sieciowych na podstawie informacji gromadzonych w oparciu o dane dostarczane przez producenta. - Program powinien chronić przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX). - Program ma mieć funkcję wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz innych narzędzi hakerskich. - Program ma mieć moduł skanujący pocztę przychodzącą i wychodzącą dla klienta poczty elektronicznej minimum Microsoft Office Outlook, który to program jest używany przez Zamawiającego. - Wbudowany moduł skanujący ruch HTTP w ma działać czasie rzeczywistym niezależnie od wykorzystywanej przez użytkowników przeglądarki WWW. - Program ma posiadać wbudowany moduł wyszukiwania heurystycznego - Program ma umożliwiać ochronę przed niebezpiecznymi rodzajami aktywności sieciowej oraz umożliwiać tworzenie reguł wykluczających dla określonych adresów/zakresów IP. - Program ma umożliwiać centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym za pośrednictwem modułu serwera oraz dostarczonego oprogramowania konsoli administratora. - Możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych. - Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. - Możliwość tworzenia list zaufanych procesów, dla których nie będzie monitorowana aktywność plikowa, aktywność aplikacji, nie będą dziedziczone ograniczenia nadrzędnego procesu, nie będzie monitorowana aktywność aplikacji potomnych, dostęp do rejestru oraz ruch sieciowy.	**TAK * / NIE ***
4.	Serwer oraz konsola zarządzania	Każdy z pakietów oprogramowania przeznaczonego zarówno na stacje robocze oraz serwery musi integrować się z konsolą zarządzania dostarczaną przez producenta oprogramowania antywirusowego. Pakiet instalacyjny systemu scentralizowanego zarządzania musi spełniać następujące wymagania:	**TAK * / NIE ***

		- System zdalnego zarządzania ma umożliwiać zarządzanie stacjami roboczymi i serwerami plików działającymi pod kontrolą systemów operacyjnych przynajmniej z rodziny Microsoft Windows/Linux posiadanych przez Zamawiającego. - Konsola administracyjna ma umożliwiać zdalne inicjowanie skanowania antywirusowego na kontrolowanych za jej pośrednictwem stacjach roboczych. - System centralnego zarządzania musi być wyposażony w mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych w sieci. - System zarządzania ma umożliwiać dystrybucję i instalowanie aktualizacji oprogramowania, który umożliwia automatyczne, przesłanie i zainstalowanie nowego oprogramowania na stacjach roboczych bez ingerencji ich użytkowników. - System musi posiadać moduł centralnego zbierania informacji i tworzenia sumarycznych raportów na temat zarejestrowanych zdarzeń. - System zdalnego zarządzania musi umożliwiać podgląd w czasie rzeczywistym statystyk ochrony, stanu aktualizacji komponentów oprogramowania antywirusowego, wykrytych zagrożeń itp. - System zdalnego zarządzania musi umożliwiać przeglądanie informacji o obiektach poddanych kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, skanowanie itp.). - System zdalnego zarządzania musi umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania. - System zdalnego zarządzania musi umożliwiać automatyczne instalowanie licencji oprogramowania antywirusowego na stacjach roboczych. - System zdalnego zarządzania powinien mieć możliwość sprawdzenia aktualnych wersji oprogramowania antywirusowego na serwerach i stacjach roboczych.	

* **Niepotrzebne skreślić**

Zestaw certyfikatów kwalifikowalnych			
Producent / Firma:		**Podać: ……**	
Urządzenie typ / model:		**Podać: ……**	
Lp.	**Parametr**	**Minimalne wymagania**	**Oferowany parametr**
1.	Certyfikaty kwalifikowalne	Zamawiający wymaga dostarczenia dla 5 osób Wydziału Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami kwalifikowanych podpisów elektronicznych na okres 2 lat wraz z kartą oraz czytnikiem lub kluczem USB	**TAK * / NIE ***

* **Niepotrzebne skreślić**

Oświadczam(y), że oferowany powyżej urządzenia posiadają i spełniają wszystkie wymagane minimalne warunki dotyczące ich konstrukcji, parametrów technicznych, jakościowych i funkcjonalnych oraz ich przeznaczenia określone w OPZ stanowiącym załacznik nr 7 do przedmiotowej Specyfikacji Istotnych Warunków Zamówienia oraz są kompletne i gotowy do użytkowania bez konieczności ponoszenia przez zamawiającego żadnych dodatkowych kosztów.

Pakiet Nr 3
Sprzęt komputerowy

3.3. ŁĄCZNA CENA OFERTOWA BRUTTO PAKIETU NR 3:

Oferuję wykonanie zamówienia w zakresie objętym przedmiotem zamówienia określonym w SIWZ w zakresie Pakietu Nr 3 do udziału w niniejszym postępowaniu za ŁĄCZNĄ CENĘ OFERTOWĄ BTUTTO *:

ŁĄCZNA CENA OFERTOWA	**..... , ... zł brutto**

Powyższa łączna cena ofertowa zawiera doliczony zgodnie z obowiązującymi w Polsce przepisami podatek VAT, który na datę złożenia oferty **wynosi ..... %**.

* ŁĄCZNA CENA OFERTOWA BRUTTO stanowi całkowite maksymalne łączne wynagrodzenie należne

wykonawcy w związku z realizacją przedmiotu niniejszego postępowania w zakresie Pakietu Nr 3 zgodnie z postanowieniami przedmiotowej SIWZ.

Oferuję dostawę następujących urządzeń spełniających wszystkie wymagania określone w OPZ do Pakietu Nr 3 (załącznik nr 8 do SIWZ) o następującej konstrukcji, parametrach technicznych, jakościowych i funkcjonalnych oraz ich przeznaczenia:

Zestaw komputerowy z oprogramowaniem, stanowisko dwumonitorowe typ 1 – 2 sztuki

Producent / Firma:	**Podać: .....**
Urządzenie typ / model:	**Podać: .....**

Lp.	Parametr	Minimalne wymagania	Oferowany parametr
1.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, Zintegrowanego Systemu Informatycznego, aplikacji obliczeniowych, aplikacji graficznych, dostępu do Internetu, poczty elektronicznej oraz przechowywania danych.	**TAK * / NIE ***
2.	Wydajność	Zamawiający oczekuje, że zaoferowane urządzenie uzyska w teście: BAPCo® SYSmark® 2014, w ramach scenariusza: „<Office Productivity>" wynik nie gorszy, niż 1400 punktów, a w ramach scenariusza „<Data/Financial Analysis>" wynik nie gorszy, niż 2000 punktów. lub BAPCo® SYSmark® 2014 SE, w ramach scenariusza: „<Office Productivity>" wynik nie gorszy, niż 900 punktów, a w ramach scenariusza „<Data/Financial Analysis>" wynik nie gorszy, niż 950 punktów.	(Podać): **TEST:** **.....** **Ilość punktów:** **.....** **Model procesora:** **.....**
3.	Pamięć RAM	Min. 8 GB.	**TAK * / NIE ***
4.	Dysk twardy SSD	2 szt. min. 240 GB, zabezpieczenie sprzętowe RAID 0/1	**TAK * / NIE *** (Podać): **Producent dysku:** **.....** **Model dysku:** **.....**
5.	Napęd optyczny	DVD-RW z oprogramowaniem do nagrywania płyt DVD.	**TAK * / NIE ***
6.	Karta dźwiękowa	TAK -w standardzie High Definition. - wbudowany głośnik do odtwarzania dźwięku.	**TAK * / NIE ***
7.	Karta sieciowa	10/100/1000 Mbps WoL, PXE, -możliwość wyłączenia karty sieciowej w BIOS.	**TAK * / NIE ***
8.	Karta graficzna	TAK	**TAK * / NIE ***
9.	Porty I/O	- 6 portów USB (2 z przodu, 4 z tyłu), - 1 port RJ-45, - 2 port DVI/Display Port/HDMI	**TAK * / NIE ***
10.	System operacyjny	Licencja na system operacyjny w najnowszej w polskiej wersji językowej bez ograniczeń czasowych wraz z dostarczonym nośnikiem. Zamawiający wymaga aby dostarczony system umożliwiał poprawną pracę obecnie użytkowanych systemów informatycznych, tj.: Vega, Microstation, Geobid. Dostarczony system operacyjny w zakresie równoważności musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; 2. Internetowa aktualizacja zapewniona w języku polskim; 3. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 4. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; 5. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); 6. Interfejs użytkownika działający w trybie graficznym, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji;	**TAK * / NIE ***

		7. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; 8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; 9. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie, aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; 10. Wbudowany system pomocy w języku polskim; 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 12. Możliwość zarządzania stacją roboczą poprzez polityki - przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; 13. Wsparcie dla logowania przy pomocy smartcard; 14. Rozbudowane polityki bezpieczeństwa - polityki dla systemu operacyjnego i dla wskazanych aplikacji; 15. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 16. Zdalna pomoc i współdzielenie aplikacji - możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; 17. Graficzne środowisko instalacji i konfiguracji; 18. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; 19. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; 20. Możliwość przywracania plików systemowych.	
11.	Oprogramowanie	Pakiet biurowy umożliwiający pracę grupową na dokumentach oraz bazach danych w formacie .mdb obecnie stosowanych przez Zamawiającego, w pełni obsługujący niniejsze bazy Zamawiającego bez utraty jakichkolwiek ich parametrów i cech użytkowych. Licencja nie może być ograniczona czasowo. Zamawiający wymaga spełnienia przez oprogramowanie minimalnych wymagań w zakresie funkcjonalności określonych poniżej: 1. Wymagania odnośnie interfejsu użytkownika: a. Pełna polska wersja językowa interfejsu użytkownika, b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. 2. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców. 3. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). 4. Do aplikacji musi być dostępna dokumentacja w języku polskim. 5. Pakiet zintegrowanych aplikacji biurowych musi zawierać: a. Edytor tekstów, b. Arkusz kalkulacyjny, c. Narzędzie do przygotowywania i prowadzenia prezentacji, d. Narzędzie do tworzenia drukowanych materiałów informacyjnych, e. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), f. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR. g. Oprogramowanie bazodanowe potrafiące odczytać pliki w formacie m.in. .mdb 6. Edytor tekstów musi umożliwiać: a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, b. Wstawianie oraz formatowanie tabel, c. Wstawianie oraz formatowanie obiektów graficznych, d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i	**TAK * / NIE ***

		rysunków, f. Automatyczne tworzenie spisów treści, g. Formatowanie nagłówków i stopek stron, h. Sprawdzanie pisowni w języku polskim, i. Śledzenie zmian wprowadzonych przez użytkowników, j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, k. Określenie układu strony (pionowa/pozioma), l. Wydruk dokumentów, m. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, o. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, 8. Arkusz kalkulacyjny musi umożliwiać: a. Tworzenie raportów tabelarycznych, b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, g. Wyszukiwanie i zamianę danych, h. Wykonywanie analiz danych przy użyciu formatowania warunkowego, i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, k. Formatowanie czasu, daty i wartości finansowych z polskim formatem l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku, m. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. 9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a. Prezentowanie przy użyciu projektora multimedialnego, b. Drukowanie w formacie umożliwiającym robienie notatek, c. Zapisanie jako prezentacja tylko do odczytu, d. Nagrywanie narracji i dołączanie jej do prezentacji, e. Opatrywanie slajdów notatkami dla prezentera, f. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, g. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, h. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, i. Możliwość tworzenia animacji obiektów i całych slajdów, j. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. 10. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: a. Tworzenie i edycję drukowanych materiałów informacyjnych, b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów, c. Edycję poszczególnych stron materiałów, d. Podział treści na kolumny, e. Umieszczanie elementów graficznych, f. wykorzystanie mechanizmu korespondencji seryjnej, g. Płynne przesuwanie elementów po całej stronie publikacji, h. Eksport publikacji do formatu PDF oraz TIFF, i. Wydruk publikacji, j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK. 11. Narzędzie do zarządzania informacją prywatną (pocztą	

		elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, b. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, c. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, d. Automatyczne grupowanie poczty o tym samym tytule, e. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, f. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, g. Zarządzanie kalendarzem i kontaktami.	
12.	Obudowa i bezpieczeństwo	Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej. Czytnik Smart Card wbudowany w obudowę lub klawiaturę.	**TAK * / NIE ***
13.	Monitor	2 szt. - LED min. 21,5" min. 1920x1080, DVI/Display Port/HDMI. Regulacja położenia wysokości ekranu. Monitory skonfigurowane do pracy dwumonitorowej.	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Jakość Dostawa monitorów o przekątnej ≥ 22,5": • Nie – 0 pkt, • Tak – 5 pkt.	**Jakość**: Dostawa monitorów o przekątnej ≥ 22,5": **TAK * / NIE *** (Podać): **…… cali**
14.	Klawiatura	Klawiatura USB w układzie US.	**TAK * / NIE ***
15.	Mysz	- Mysz laserowa - USB - czteroprzyciskowa.	**TAK * / NIE ***
16.	Dodatki	Patchcord RJ-45, długość 2 metry.	**TAK * / NIE ***
17.	Gwarancja	Gwarancja min. 36 miesięcy na zestaw, reakcja serwisu następnego dnia roboczego po zgłoszeniu. Dysk twardy pozostaje u Zamawiającego.	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Gwarancja Wydłużenie okresu gwarancji: • Gwarancja: 36 miesięcy – 0 pkt, • Gwarancja: 37 – 44 miesięcy – 1 pkt, • Gwarancja: 45 – 50 miesięcy – 2 pkt, • Gwarancja: 51 – 55 miesięcy – 3 pkt, • Gwarancja: 56 – 59 miesięcy – 4 pkt, • Gwarancja: 60 miesięcy – 5 pkt,	**Gwarancja** (Podać): **…… m-cy**
18.	Certyfikaty i normy	1. Maksymalnie 28 dB z pozycji operatora w trybie IDLE, 2. Deklaracja zgodności CE, 3. Certyfikaty jakości ISO 9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność	
19.	Stan	Fabrycznie nowy	**TAK * / NIE ***

*** Niepotrzebne skreślić**

Zestaw komputerowy z oprogramowaniem, stanowisko dwumonitorowe typ 2 – 3 sztuki

Producent / Firma:		**Podać: ……**	
Urządzenie typ / model:		**Podać: ……**	
Lp.	**Parametr**	**Minimalne wymagania**	**Oferowany parametr**
1.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, Zintegrowanego Systemu Informatycznego, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej.	**TAK * / NIE ***
2.	Wydajność	Zamawiający oczekuje, że zaoferowane urządzenie uzyska w teście: BAPCo® SYSmark® 2014, w ramach scenariusza: „<Office Productivity>" wynik nie gorszy, niż 1300 punktów, a w ramach scenariusza „<Data/Financial Analysis>" wynik nie gorszy, niż 1700 punktów. lub BAPCo® SYSmark® 2014 SE, w ramach scenariusza: „<Office Productivity>" wynik nie gorszy, niż 800 punktów, a w ramach scenariusza „<Data/Financial Analysis>" wynik nie gorszy, niż 950	Podać): **TEST:** **……** **Ilość punktów:** **……** **Model procesora:**

		punktów.	.....
3.	Pamięć RAM	Min. 8 GB.	**TAK * / NIE ***
4.	Dysk twardy SSD	Min. 120 GB	**TAK * / NIE *** (Podać): **Producent dysku:** ..... **Model dysku:** .....
5.	Napęd optyczny	DVD-RW z oprogramowaniem do nagrywania płyt DVD.	**TAK * / NIE ***
6.	Karta dźwiękowa	TAK - w standardzie High Definition. - wbudowany głośnik do odtwarzania dźwięku.	**TAK * / NIE ***
7.	Karta sieciowa	10/100/1000 Mbps WoL, PXE, - możliwość wyłączenia karty sieciowej w BIOS.	**TAK * / NIE ***
8.	Karta graficzna	TAK	**TAK * / NIE ***
9.	Porty I/O	- 6 portów USB (2 z przodu, 4 z tyłu), - 1 port RJ-45, - 2 port DVI/Display Port/HDMI	**TAK * / NIE ***
10.	System operacyjny	Licencja na system operacyjny w najnowszej w polskiej wersji językowej bez ograniczeń czasowych wraz z dostarczonym nośnikiem. Zamawiający wymaga aby dostarczony system umożliwiał poprawną pracę obecnie użytkowanych systemów informatycznych, tj.: Vega, Microstation, Geobid. Dostarczony system operacyjny w zakresie równoważności musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; 2. Internetowa aktualizacja zapewniona w języku polskim; 3. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 4. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; 5. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); 6. Interfejs użytkownika działający w trybie graficznym, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji; 7. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; 8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; 9. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie, aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; 10. Wbudowany system pomocy w języku polskim; 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 12. Możliwość zarządzania stacją roboczą poprzez polityki - przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; 13. Wsparcie dla logowania przy pomocy smartcard; 14. Rozbudowane polityki bezpieczeństwa - polityki dla systemu operacyjnego i dla wskazanych aplikacji; 15. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 16. Zdalna pomoc i współdzielenie aplikacji - możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; 17. Graficzne środowisko instalacji i konfiguracji; 18. Zarządzanie kontami użytkowników sieci oraz urządzeniami	**TAK * / NIE ***

		sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; 19. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; 20. Możliwość przywracania plików systemowych.	
11.	Oprogramowanie	Pakiet biurowy umożliwiający pracę grupową na dokumentach oraz bazach danych w formacie .mdb obecnie stosowanych przez Zamawiającego, w pełni obsługujący niniejsze bazy Zamawiającego bez utraty jakichkolwiek ich parametrów i cech użytkowych. Licencja nie może być ograniczona czasowo. Zamawiający wymaga spełnienia przez oprogramowanie minimalnych wymagań w zakresie funkcjonalności określonych poniżej: 1. Wymagania odnośnie interfejsu użytkownika: a. Pełna polska wersja językowa interfejsu użytkownika, b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. 2. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców. 3. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). 4. Do aplikacji musi być dostępna dokumentacja w języku polskim. 5. Pakiet zintegrowanych aplikacji biurowych musi zawierać: a. Edytor tekstów, b. Arkusz kalkulacyjny, c. Narzędzie do przygotowywania i prowadzenia prezentacji, d. Narzędzie do tworzenia drukowanych materiałów informacyjnych, e. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), f. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR. g. Oprogramowanie bazodanowe potrafiące odczytać pliki w formacie m.in. .mdb 6. Edytor tekstów musi umożliwiać: a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, b. Wstawianie oraz formatowanie tabel, c. Wstawianie oraz formatowanie obiektów graficznych, d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, f. Automatyczne tworzenie spisów treści, g. Formatowanie nagłówków i stopek stron, h. Sprawdzanie pisowni w języku polskim, i. Śledzenie zmian wprowadzonych przez użytkowników, j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, k. Określenie układu strony (pionowa/pozioma), l. Wydruk dokumentów, m. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, o. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, 8. Arkusz kalkulacyjny musi umożliwiać: a. Tworzenie raportów tabelarycznych, b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie	**TAK * / NIE ***

		problemów optymalizacyjnych f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, g. Wyszukiwanie i zamianę danych, h. Wykonywanie analiz danych przy użyciu formatowania warunkowego, i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, k. Formatowanie czasu, daty i wartości finansowych z polskim formatem l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku, m. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. 9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a. Prezentowanie przy użyciu projektora multimedialnego, b. Drukowanie w formacie umożliwiającym robienie notatek, c. Zapisanie jako prezentacja tylko do odczytu, d. Nagrywanie narracji i dołączanie jej do prezentacji, e. Opatrywanie slajdów notatkami dla prezentera, f. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, g. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, h. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, i. Możliwość tworzenia animacji obiektów i całych slajdów, j. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. 10. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: a. Tworzenie i edycję drukowanych materiałów informacyjnych, b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów, c. Edycję poszczególnych stron materiałów, d. Podział treści na kolumny, e. Umieszczanie elementów graficznych, f. wykorzystanie mechanizmu korespondencji seryjnej, g. Płynne przesuwanie elementów po całej stronie publikacji, h. Eksport publikacji do formatu PDF oraz TIFF, i. Wydruk publikacji, j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK. 11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, b. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, c. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, d. Automatyczne grupowanie poczty o tym samym tytule, e. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, f. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, g. Zarządzanie kalendarzem i kontaktami.	
12.	Obudowa i bezpieczeństwo	Typu nabiurkowa mało gabarytowa, z przeznaczeniem na montaż na biurku w pozycji poziomej. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej. Czytnik Smart Card wbudowany w obudowę lub klawiaturę.	**TAK * / NIE ***
13.	Monitor	2 szt. - LED min. 21,5" min. 1920x1080, DVI/Display Port/HDMI. Regulacja położenia wysokości ekranu. Monitory skonfigurowane do pracy dwumonitorowej.	**TAK * / NIE ***
14.	Klawiatura	Klawiatura USB w układzie US.	**TAK * / NIE ***
15.	Mysz	- Mysz laserowa - USB - czteroprzyciskowa.	**TAK * / NIE ***
16.	Dodatki	Patchcord RJ-45, długość 2 metry.	**TAK * / NIE ***

17.	Gwarancja	Gwarancja min. 36 miesięcy na zestaw, reakcja serwisu następnego dnia roboczego po zgłoszeniu. Dysk twardy pozostaje u Zamawiającego.	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Gwarancja Wydłużenie okresu gwarancji: • Gwarancja: 36 miesięcy – 0 pkt, • Gwarancja: 37 – 44 miesięcy – 2 pkt, • Gwarancja: 45 – 50 miesięcy – 4 pkt, • Gwarancja: 51 – 55 miesięcy – 6 pkt, • Gwarancja: 56 – 59 miesięcy – 8 pkt, • Gwarancja: 60 miesięcy – 10 pkt,	**Gwarancja** (Podać): **..... m-cy**
18.	Certyfikaty i normy	1. Maksymalnie 28 dB z pozycji operatora w trybie IDLE, 2. Deklaracja zgodności CE, 3. Certyfikaty jakości ISO 9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność	**TAK * / NIE ***
19.	Stan	Fabrycznie nowy	**TAK * / NIE ***

*** Niepotrzebne skreślić**

Zestaw komputerowy z oprogramowaniem, stanowisko dwumonitorowe typ 3 – 10 sztuk

Producent / Firma:	**Podać: .....**
Urządzenie typ / model:	**Podać: .....**

Lp.	Parametr	Minimalne wymagania	Oferowany parametr
1.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, Zintegrowanego Systemu Informatycznego, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej.	**TAK * / NIE ***
2.	Wydajność	Zamawiający oczekuje, że zaoferowane urządzenie uzyska w teście: BAPCo® SYSmark® 2014, w ramach scenariusza: „<Office Productivity>" wynik nie gorszy, niż 1300 punktów, a w ramach scenariusza „<Data/Financial Analysis>" wynik nie gorszy, niż 1700 punktów. lub BAPCo® SYSmark® 2014 SE, w ramach scenariusza: „<Office Productivity>" wynik nie gorszy, niż 800 punktów, a w ramach scenariusza „<Data/Financial Analysis>" wynik nie gorszy, niż 950 punktów.	(Podać): **TEST:** **.....** **Ilość punktów:** **.....** **Model procesora:** **.....**
3.	Pamięć RAM	Min. 8 GB.	**TAK * / NIE ***
4.	Dysk twardy SSD	Min. 120 GB	**TAK * / NIE *** (Podać): **Producent dysku:** **.....** **Model dysku:** **.....**
5.	Napęd optyczny	DVD-RW z oprogramowaniem do nagrywania płyt DVD.	**TAK * / NIE ***
6.	Karta dźwiękowa	TAK - w standardzie High Definition. - wbudowany głośnik do odtwarzania dźwięku.	**TAK * / NIE ***
7.	Karta sieciowa	10/100/1000 Mbps WoL, PXE, - możliwość wyłączenia karty sieciowej w BIOS.	**TAK * / NIE ***
8.	Karta graficzna	TAK	**TAK * / NIE ***
9.	Porty I/O	- 6 portów USB (2 z przodu, 4 z tyłu), - 1 port RJ-45, - 2 port DVI/Display Port/HDMI	**TAK * / NIE ***
10.	System operacyjny	Licencja na system operacyjny w najnowszej w polskiej wersji językowej bez ograniczeń czasowych wraz z dostarczonym nośnikiem. Zamawiający wymaga aby dostarczony system umożliwiał poprawną pracę obecnie użytkowanych systemów informatycznych, tj.: Vega, Microstation, Geobid. Dostarczony system operacyjny w zakresie równoważności musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Możliwość dokonywania aktualizacji i poprawek systemu przez	**TAK * / NIE ***

		Internet z możliwością wyboru instalowanych poprawek; 2. Internetowa aktualizacja zapewniona w języku polskim; 3. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 4. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; 5. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); 6. Interfejs użytkownika działający w trybie graficznym, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji; 7. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; 8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; 9. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie, aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; 10. Wbudowany system pomocy w języku polskim; 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 12. Możliwość zarządzania stacją roboczą poprzez polityki - przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; 13. Wsparcie dla logowania przy pomocy smartcard; 14. Rozbudowane polityki bezpieczeństwa - polityki dla systemu operacyjnego i dla wskazanych aplikacji; 15. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 16. Zdalna pomoc i współdzielenie aplikacji - możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; 17. Graficzne środowisko instalacji i konfiguracji; 18. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; 19. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; 20. Możliwość przywracania plików systemowych.	
11.	Oprogramowanie	Pakiet biurowy umożliwiający pracę grupową na dokumentach . Licencja nie może być ograniczona czasowo. Zamawiający wymaga spełnienia przez oprogramowanie minimalnych wymagań w zakresie funkcjonalności określonych poniżej: 1. Wymagania odnośnie interfejsu użytkownika: a. Pełna polska wersja językowa interfejsu użytkownika, b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. 2. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców. 3. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). 4. Do aplikacji musi być dostępna dokumentacja w języku polskim. 5. Pakiet zintegrowanych aplikacji biurowych musi zawierać: a. Edytor tekstów, b. Arkusz kalkulacyjny, c. Narzędzie do przygotowywania i prowadzenia prezentacji, d. Narzędzie do tworzenia drukowanych materiałów informacyjnych, e. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), f. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR. 6. Edytor tekstów musi umożliwiać: a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą	**TAK * / NIE ***

		języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, b. Wstawianie oraz formatowanie tabel, c. Wstawianie oraz formatowanie obiektów graficznych, d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, f. Automatyczne tworzenie spisów treści, g. Formatowanie nagłówków i stopek stron, h. Sprawdzanie pisowni w języku polskim, i. Śledzenie zmian wprowadzonych przez użytkowników, j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, k. Określenie układu strony (pionowa/pozioma), l. Wydruk dokumentów, m. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, o. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, 8. Arkusz kalkulacyjny musi umożliwiać: a. Tworzenie raportów tabelarycznych, b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, g. Wyszukiwanie i zamianę danych, h. Wykonywanie analiz danych przy użyciu formatowania warunkowego, i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, k. Formatowanie czasu, daty i wartości finansowych z polskim formatem l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku, n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. 9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a. Prezentowanie przy użyciu projektora multimedialnego, b. Drukowanie w formacie umożliwiającym robienie notatek, c. Zapisanie jako prezentacja tylko do odczytu, d. Nagrywanie narracji i dołączanie jej do prezentacji, e. Opatrywanie slajdów notatkami dla prezentera, f. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, g. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, h. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, i. Możliwość tworzenia animacji obiektów i całych slajdów, j. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. 10. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: a. Tworzenie i edycję drukowanych materiałów informacyjnych, b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów, c. Edycję poszczególnych stron materiałów, d. Podział treści na kolumny,	

		e. Umieszczanie elementów graficznych, f. wykorzystanie mechanizmu korespondencji seryjnej, g. Płynne przesuwanie elementów po całej stronie publikacji, h. Eksport publikacji do formatu PDF oraz TIFF, i. Wydruk publikacji, j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK. 11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, b. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, c. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, d. Automatyczne grupowanie poczty o tym samym tytule, e. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, f. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, g. Zarządzanie kalendarzem i kontaktami.	
12.	Obudowa i bezpieczeństwo	Typu nabiurkowa mało gabarytowa, z przeznaczeniem na montaż na biurku w pozycji poziomej. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej. Czytnik Smart Card wbudowany w obudowę lub klawiaturę.	**TAK * / NIE ***
13.	Monitor	2 szt. - LED min. 21,5" min. 1920x1080, DVI/Display Port/HDMI. Regulacja położenia wysokości ekranu. Monitory skonfigurowane do pracy dwumonitorowej.	**TAK * / NIE ***
14.	Klawiatura	Klawiatura USB w układzie US.	**TAK * / NIE ***
15.	Mysz	- Mysz laserowa - USB - czteroprzyciskowa.	**TAK * / NIE ***
16.	Dodatki	Patchcord RJ-45, długość 2 metry.	**TAK * / NIE ***
17.	Gwarancja	Gwarancja min. 36 miesięcy na zestaw, reakcja serwisu następnego dnia roboczego po zgłoszeniu. Dysk twardy pozostaje u Zamawiającego.	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Gwarancja Wydłużenie okresu gwarancji: • Gwarancja: 36 miesięcy – 0 pkt, • Gwarancja: 37 – 44 miesięcy – 2 pkt, • Gwarancja: 45 – 50 miesięcy – 4 pkt, • Gwarancja: 51 – 55 miesięcy – 6 pkt, • Gwarancja: 56 – 59 miesięcy – 8 pkt, • Gwarancja: 60 miesięcy – 10 pkt,	**Gwarancja** (Podać): **..... m-cy**
18.	Certyfikaty i normy	1. Maksymalnie 28 dB z pozycji operatora w trybie IDLE, 2. Deklaracja zgodności CE, 3. Certyfikaty jakości ISO 9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność	**TAK * / NIE ***
19.	Stan	Fabrycznie nowy	**TAK * / NIE ***

*** Niepotrzebne skreślić**

Terminal komputerowy dwumonitorowy – 6 sztuk

Producent / Firma:	**Podać: ……**
Urządzenie typ / model:	**Podać: ……**

Lp.	Parametr	Minimalne wymagania	Oferowany parametr
1.	Zastosowanie	Terminal będzie wykorzystywany dla potrzeb aplikacji biurowych, Zintegrowanego Systemu Informatycznego, oprogramowania typu CAD, dostępu do internetu oraz poczty elektronicznej. Niniejsze urządzenie powinno zapewniać płynną i komfortową pracę użytkowników w powyższych zastosowaniach.	**TAK * / NIE ***
2.	Procesor	Procesor dedykowany do niniejszego rozwiązania	**TAK * / NIE ***
3.	Pamięć flash	Min. 8 GB	**TAK * / NIE ***

4.	Pamięć RAM	Min 2 GB	**TAK * / NIE ***
5.	Karta dźwiękowa	Zintegrowana	**TAK * / NIE ***
6.	Karta sieciowa	LAN - Zintegrowana 10/100/1000 z obsługą Wake-on-Lan.	**TAK * / NIE ***
		UWAGA – parametr służący wyłącznie ocenie ofert w kryterium wyboru oferty – Jakość WiFi – Zintegrowana b/g/n: • Nie – 0 pkt, • Tak – 5 pkt.	**Jakość**: WiFi – Zintegrowana b/g/n: **TAK * / NIE ***
7.	Karta graficzna	TAK, obsługa dwumonitorowa min. rozdzielczość FULL HD.	**TAK * / NIE ***
8.	Porty I/O	Minimum 4 x USB 2.0 w tym 2 USB na panelu przednim, 1 x RJ-45, 2 x DVI/DisplayPort/HDMI, 1 x wyjście liniowe (słuchawki/głośnik).	**TAK * / NIE ***
9.	Wsparcie dla protokołów	PCoIP, RDP	**TAK * / NIE ***
10.	Obudowa	Możliwość pracy w pozycji pionowej (dostarczenie podstawki) i poziomej Możliwość montażu ściennego w standardzie VESA 100x100mm Czytnik Smart Card wbudowany w obudowę lub klawiaturę.	**TAK * / NIE ***
11.	Monitor	2 szt. - LED min. 21,5" min. 1920x1080, DVI/Display Port/HDMI. Regulacja położenia wysokości ekranu. Monitory skonfigurowane do pracy dwumonitorowej.	**TAK * / NIE ***
12.	Klawiatura	Klawiatura USB w układzie QWERTY.	**TAK * / NIE ***
13.	Mysz	Mysz optyczna USB. Dwu-przyciskowa, rolka (scroll).	**TAK * / NIE ***
14.	Zarządzanie:	Zdalne zarządzanie, inwentaryzacja, konfiguracja terminala z wykorzystaniem dołączonego oprogramowania producenta. Zdalne przejmowanie ekranu na terminalu.	**TAK * / NIE ***
15.	System operacyjny	Licencja na system operacyjny bez ograniczeń czasowych. Zamawiający wymaga aby dostarczony system umożliwiał uzyskanie sesji terminalowej na serwerze z wykorzystaniem protokołów PCoIP, RDP. System ma umożliwiać poprawną pracę z wykorzystaniem środowiska dwumonitorowego oraz uwierzytelniania użytkownika z wykorzystaniem czytników oraz kart smart card.	**TAK * / NIE ***
16.	Gwarancja	Gwarancja min. 36 miesięcy na zestaw, reakcja serwisu następnego dnia roboczego po zgłoszeniu.	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Gwarancja Wydłużenie okresu gwarancji: • Gwarancja: 36 miesięcy – 0 pkt, • Gwarancja: 37 – 44 miesięcy – 1 pkt, • Gwarancja: 45 – 50 miesięcy – 2 pkt, • Gwarancja: 51 – 55 miesięcy – 3 pkt, • Gwarancja: 56 – 59 miesięcy – 4 pkt, • Gwarancja: 60 miesięcy – 5 pkt,	**Gwarancja** (Podać): **…… m-cy**
17.	Certyfikaty i normy	1. Deklaracja zgodności CE, 2. Certyfikaty jakości ISO 9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność	**TAK * / NIE ***
18.	Stan	Fabrycznie nowy	**TAK * / NIE ***

*** Niepotrzebne skreślić**

Zestaw do bezpiecznego uwierzytelniania

Producent / Firma:	**Podać: ……**
Urządzenie typ / model:	**Podać: ……**

Lp.	Parametr	Minimalne wymagania	Oferowany parametr
1.	Zestaw do bezpiecznego uwierzytelniania	Zamawiający wymaga dostarczenia 30 zestawów do logowania w systemie (czytnik smard card oraz karta smard card procesorowa). Wraz z zestawem jest wymagane oprogramowanie umożliwiające poprawne logowanie się użytkowników do stacji roboczych (komputerów oraz terminali) z wykorzystaniem Active Directory.	**TAK * / NIE ***

*** Niepotrzebne skreślić**

Oświadczam(y), że oferowany powyżej urządzenia posiadają i spełniają wszystkie wymagane minimalne warunki dotyczące ich konstrukcji, parametrów technicznych, jakościowych i funkcjonalnych oraz ich przeznaczenia określone w OPZ stanowiącym załacznik nr 8 do przedmiotowej Specyfikacji Istotnych Warunków Zamówienia oraz są kompletne i gotowy do użytkowania bez konieczności ponoszenia przez zamawiającego żadnych dodatkowych kosztów.

Pakiet Nr 4
UPS-y i przenośne stacje robocze

3.4. ŁĄCZNA CENA OFERTOWA BRUTTO PAKIETU NR 4:

Oferuję wykonanie zamówienia w zakresie objętym przedmiotem zamówienia określonym w SIWZ w zakresie Pakietu Nr 4 do udziału w niniejszym postępowaniu za ŁĄCZNĄ CENĘ OFERTOWĄ BTUTTO *:

ŁĄCZNA CENA OFERTOWA	**..... , ... zł brutto**

Powyższa łączna cena ofertowa zawiera doliczony zgodnie z obowiązującymi w Polsce przepisami podatek VAT, który na datę złożenia oferty **wynosi ..... %**.

* ŁĄCZNA CENA OFERTOWA BRUTTO stanowi całkowite maksymalne łączne wynagrodzenie należne wykonawcy w związku z realizacją przedmiotu niniejszego postępowania w zakresie Pakietu Nr 4 zgodnie z postanowieniami przedmiotowej SIWZ.

Oferuję dostawę następujących urządzeń spełniających wszystkie wymagania określone w OPZ do Pakietu Nr 4 (załącznik nr 9 do SIWZ) o następującej konstrukcji, parametrach technicznych, jakościowych i funkcjonalnych oraz ich przeznaczenia:

Zasilacz awaryjny (UPS) – 18 sztuk

Producent / Firma:	**Podać: .....**
Urządzenie typ / model:	**Podać: .....**

Lp.	Parametr	Minimalne wymagania	Oferowany parametr
1.	Moc	Min. 700VA	**TAK * / NIE ***
2.	Technologia	Line-interactive	**TAK * / NIE ***
3.	Komunikacja	1 port USB	**TAK * / NIE ***
4.	AVR	TAK	**TAK * / NIE ***
5.	Standardowy czas zasilania awaryjnego zasilacza	8 minut	**TAK * / NIE ***
6.	Gwarancja	Min. 24 miesiące	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Gwarancja Wydłużenie okresu gwarancji: • Gwarancja: 24 miesiące – 0 pkt, • Gwarancja: 25 – 27 miesięcy – 2 pkt, • Gwarancja: 28 – 30 miesięcy – 4 pkt, • Gwarancja: 31 – 33 miesięcy – 6 pkt, • Gwarancja: 34 – 35 miesięcy – 8 pkt, • Gwarancja: 36 miesięcy – 10 pkt,	**Gwarancja** (Podać): **..... m-cy**
7.	Certyfikaty i normy	1. Deklaracja zgodności CE, 2. Certyfikaty jakości ISO 9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność	**TAK * / NIE ***
8.	Stan	Fabrycznie nowy	**TAK * / NIE ***

* **Niepotrzebne skreślić**

Przenośna stacja robocza – 2 sztuki

Producent / Firma:		**Podać: ……**	
Urządzenie typ / model:		**Podać: ……**	
Lp.	**Parametr**	**Minimalne wymagania**	**Oferowany parametr**
1.	Zastosowanie	Komputer będzie wykorzystywany jako stanowisko mobilne dla potrzeb aplikacji biurowych, Zintegrowanego Systemu Informatycznego, aplikacji obliczeniowych, dostępu do internetu poczty elektronicznej oraz zdalnego zarządzania.	**TAK * / NIE ***
2.	Wydajność	Zamawiający oczekuje, że zaoferowane urządzenie uzyska w teście: BAPCo® SYSmark® 2014, w ramach scenariusza: „<Office Productivity>" wynik nie gorszy, niż 1000 punktów, a w ramach scenariusza „<Data/Financial Analysis>" wynik nie gorszy, niż 1100 punktów. lub BAPCo® MobileMark 2014, w ramach scenariusza: „<Office Productivity>" wynik nie gorszy, niż 1500 punktów.	(Podać): **TEST:** **……** **Ilość punktów:** **……** **Model procesora:** **……**
3.	Pamięć operacyjna	Min. 8 GB	**TAK * / NIE ***
4.	Dysk twardy SSD	Min. 128 GB	**TAK * / NIE *** (Podać): **Producent dysku:** **……** **Model dysku:** **……**
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Jakość Min. 256 GB: • Nie – 0 pkt, • Tak – 10 pkt.	**Jakość**: Min. 256 GB: **TAK * / NIE ***
5.	Wyświetlacz	Matryca 12,5 – 14" z podświetleniem w technologii LED, rozdzielczość min. FULL HD, dotykowy, ekran konwertowany w układzie tabletu	**TAK * / NIE ***
6.	Karta grafiki	TAK	**TAK * / NIE ***
7.	Karta dźwiękowa i inne wyposażenie	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo, wbudowany mikrofon, wbudowana kamera	**TAK * / NIE ***
8.	Porty wejścia/wyjścia	3 x USB w tym przynajmniej 1 x 3.0, złącze słuchawek, złącze mikrofonu, HDMI, RJ-45, czytnik kart multimedialnych	**TAK * / NIE ***
9.	Komunikacja przewodowa	Zintegrowana karta sieciowa 10/100/1000 MBit/s LAN	**TAK * / NIE ***
10.	Komunikacja bezprzewodowa	Wbudowana karta sieciowa, pracująca w standardzie b/g/n, moduł Bluetooth zintegrowany w obudowie	**TAK * / NIE ***
11.	Klawiatura	Klawiatura odporna na zalanie, układ US, podświetlanie klawiatury	**TAK * / NIE ***
12.	Zasilanie	bateria pozwalająca na nieprzerwaną pracę urządzenia min. 5 godzin	**TAK * / NIE ***
13.	Modem WWAN	**UWAGA – parametr służący wyłącznie ocenie ofert w kryterium wyboru oferty – Jakość** Min. 3G lub LTE: • Nie – 0 pkt, • Tak – 10 pkt.	**Jakość**: Min. 3G lub LTE: **TAK * / NIE ***
14.	System operacyjny	Licencja na system operacyjny w najnowszej w polskiej wersji językowej bez ograniczeń czasowych. Dostarczony system operacyjny musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; 2. Internetowa aktualizacja zapewniona w języku polskim; 3. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 4. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; 5. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi);	**TAK * / NIE ***

		6. Interfejs użytkownika działający w trybie graficznym, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji; 7. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; 8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; 9. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie, aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; 10. Wbudowany system pomocy w języku polskim;	
15.	Masa z baterią	Waga urządzenia z baterią max 1,5 kg,	**TAK * / NIE ***
16.	Torba	Futerał dedykowany do niniejszego modelu	**TAK * / NIE ***
17.	Gwarancja	Min. 24 miesiące	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Gwarancja Wydłużenie okresu gwarancji: • Gwarancja: 24 miesiące – 0 pkt, • Gwarancja: 25 – 27 miesięcy – 2 pkt, • Gwarancja: 28 – 30 miesięcy – 4 pkt, • Gwarancja: 31 – 33 miesięcy – 6 pkt, • Gwarancja: 34 – 35 miesięcy – 8 pkt, • Gwarancja: 36 miesięcy – 10 pkt,	**Gwarancja** (Podać): **…… m-cy**
18.	Certyfikaty i normy	1. Deklaracja zgodności CE, 2. Certyfikaty jakości ISO 9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność	**TAK * / NIE ***
19.	Stan	Fabrycznie nowy	**TAK * / NIE ***

* **Niepotrzebne skreślić**

Oświadczam(y), że oferowany powyżej urządzenia posiadają i spełniają wszystkie wymagane minimalne warunki dotyczące ich konstrukcji, parametrów technicznych, jakościowych i funkcjonalnych oraz ich przeznaczenia określone w OPZ stanowiącym załacznik nr 9 do przedmiotowej Specyfikacji Istotnych Warunków Zamówienia oraz są kompletne i gotowy do użytkowania bez konieczności ponoszenia przez zamawiającego żadnych dodatkowych kosztów.

Pakiet Nr 5
Skaner

3.5. ŁĄCZNA CENA OFERTOWA BRUTTO PAKIETU NR 5:

Oferuję wykonanie zamówienia w zakresie objętym przedmiotem zamówienia określonym w SIWZ w zakresie Pakietu Nr 5 do udziału w niniejszym postępowaniu za ŁĄCZNĄ CENĘ OFERTOWĄ BTUTTO *:

ŁĄCZNA CENA OFERTOWA	**…… , ….. zł brutto**

Powyższa łączna cena ofertowa zawiera doliczony zgodnie z obowiązującymi w Polsce przepisami podatek VAT, który na datę złożenia oferty **wynosi …… %**.

* ŁĄCZNA CENA OFERTOWA BRUTTO stanowi całkowite maksymalne łączne wynagrodzenie należne wykonawcy w związku z realizacją przedmiotu niniejszego postępowania w zakresie Pakietu Nr 5 zgodnie z postanowieniami przedmiotowej SIWZ.

Oferuję dostawę następujących urządzeń spełniających wszystkie wymagania określone w OPZ do Pakietu Nr 5 (załącznik nr 10 do SIWZ) o następującej konstrukcji, parametrach technicznych, jakościowych i funkcjonalnych oraz ich przeznaczenia:

Skaner – 1 sztuka	
Producent / Firma:	**Podać: ……**

Urządzenie typ / model:		**Podać: ……**	
Lp.	**Parametr**	**Minimalne wymagania**	**Oferowany parametr**
1.	Zastosowanie	Skaner będzie stanowił jako kompletny system do archiwizacji operatów technicznych z państwowego zasobu geodezyjnego i kartograficznego, jak również innych dokumentów skanowanych w Wydziale Geodezji Kartografii, Katastru i Gospodarki Nieruchomościami. Skaner musi być wyposażony w system zarządzania skanowanych dokumentów, mający na celu przyspieszenie i zwiększenie funkcjonalności pracy.	**TAK * / NIE ***
2.	Wielkość	A3	**TAK * / NIE ***
3.	Prędkość skanowania	Min. 100 arkuszy A4/min.	**TAK * / NIE ***
4.	Rozdzielczość optyczna	Min. 600 DPI	**TAK * / NIE ***
5.	Format wyjściowy	Kolor 24 Bit, skala szarości 8 Bit, monochromatyczny 1 Bit	**TAK * / NIE ***
6.	Automatyczny podajnik dokumentów	Pojemność min. 100 arkuszy	**TAK * / NIE ***
7.	Obsługiwane formaty wejściowe dokumentu	Min. A3, A4, A5, B4, B5	**TAK * / NIE ***
8.	Gramatura obsługiwanego papieru	52 - 300 g/m²	**TAK * / NIE ***
9.	Dysk twardy	Min. 250 GB	**TAK * / NIE ***
10.	Funkcje	Bezpośrednie skanowanie do emaila, na dysk twardy, do pamięci USB/SD oraz do folderu z poziomu urządzenia. Możliwość personalizacji panelu głównego oraz możliwość dopasowania panelu pod wymagania poszczególnych użytkowników (własne ikony, logo firmy itp. personalizacja) Podgląd skanów przed ich wysłaniem - z poziomu urządzenia Szyfrowanie dysku głównego w urządzeniu oraz bezpieczne nadpisywanie danych istniejących na dysku twardym urządzenia Wymagana autoryzacja na urządzeniu (kody PIN) Możliwość skanowania z rozpoznawaniem kodów kreskowych i rozpoznawaniem numeru operatu Moduł OCR pozwala na wyszukanie frazy w dokumencie PDF Skanowanie do excela, worda, pdf „przeszukiwalnego” (OCR) Skanowanie wg zdefiniowanych typów dokumentów (wg sygnatur dokumentacji technicznej – w tym zgodnie z Rozp. MAiC ws. organizacji i trybu prowadzenia państwowego zasobu geodezyjnego i kartograficznego) i automatyczne indeksowanie plików w celu integracji z bazami danych (pozwala na automatyczne zasilenie zeskanowanymi rysunkami technicznymi / mapami dowolnej bazy danych). Skanowanie na dowolnym urządzeniu, zapis pliku w jednym katalogu (wg identyfikatora zgłoszenia pracy geodezyjnej, np. KERG) Skanowanie operatów wg identyfikatorów zgłoszenia, jeden plik pdf wielostronicowy lub wiele plików pdf jednostronicowych Różne typy dokumentów mogą mieć różne parametry skanowania (wg potrzeb użytkownika – możliwość konfiguracji)	**TAK * / NIE ***
11.	Oprogramowanie	Oprogramowanie do automatycznej archiwizacji i zaawansowanej edycji dokumentacji technicznej (kalibracja i czyszczenie szumów pikselowych)	**TAK * / NIE ***
12.	Dodatkowe funkcjonalności	**UWAGA – parametr służący wyłącznie ocenie ofert w kryterium wyboru oferty – Jakość** Skaner posiadający funkcje drukowania/kopiowania o cechach: Posiada serwer dokumentów, który umożliwia drukowanie dokumentów wprost z dysku twardego urządzenia. Drukuje bezpośrednio z dysku twardego urządzenia, pendrive i karty SD (format pdf, jpg i tiff) Prędkość druku: mono/kolor – nie mniejsza niż 30 arkusze A4 /min Technologia druku laserowa kolorowa Język drukarki: PCL5c, PCL6(XL), PDF Podajnik papieru: min. 2 – kasety (A4 i A3) oraz podajnik boczny • Nie – 0 pkt, • Tak – 30 pkt.	**Jakość**: Skaner posiadający funkcje drukowania/kopiowania o opisanych cechach: **TAK * / NIE ***
13.	Mobilność	TAK, podstawa wyposażona w kółka	**TAK * / NIE ***

14.	Interfejsy	Gniazdo SD, USB Host, Ethernet 10/100/1000	**TAK * / NIE ***
15.	Gwarancja	Gwarancja min. 36 miesięcy.	**TAK * / NIE ***
		UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Gwarancja Wydłużenie okresu gwarancji: • Gwarancja: 36 miesięcy – 0 pkt, • Gwarancja: 37 – 44 miesięcy – 2 pkt, • Gwarancja: 45 – 50 miesięcy – 4 pkt, • Gwarancja: 51 – 55 miesięcy – 6 pkt, • Gwarancja: 56 – 59 miesięcy – 8 pkt, • Gwarancja: 60 miesięcy – 10 pkt,	**Gwarancja** (Podać): **…… m-cy**
16.	Certyfikaty i normy	1. Deklaracja zgodności CE, 2. Certyfikaty jakości ISO 9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność	**TAK * / NIE ***
17.	Stan	Fabrycznie nowy	**TAK * / NIE ***

* **Niepotrzebne skreślić**

Oświadczam(y), że oferowany powyżej urządzenia posiadają i spełniają wszystkie wymagane minimalne warunki dotyczące ich konstrukcji, parametrów technicznych, jakościowych i funkcjonalnych oraz ich przeznaczenia określone w OPZ stanowiącym załacznik nr 10 do przedmiotowej Specyfikacji Istotnych Warunków Zamówienia oraz są kompletne i gotowy do użytkowania bez konieczności ponoszenia przez zamawiającego żadnych dodatkowych kosztów.

4. OBOWIĄZEK PODATKOWY:

Oświadczam(y), że zgodnie z postanowieniami art. 91 ust. 3a ustawy PZP oraz punktu 19.3 SIWZ wybór niniejszej oferty **nie prowadzi* / prowadzi*** do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług (tzw. odwrócony podatek VAT).

* Niepotrzebne skreślić

Jeżeli wybór niniejszej oferty prowadziłby do powstania u zamawiającego obowiązku podatkowego wykonawcy są zobowiązani wypełnić poniższą cześć niniejszego punktu.

Jednocześnie wskazuję nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, oraz wskazując ich wartość bez kwoty podatku: ……
……
……

W przypadku jeżeli wybór niniejszej oferty prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, wykonawca składając ofertę cenową (o ktrej mowa na wstępie niniejszego punktu, tj. łączną cenę ofertową brutto (poszczególnych Pakietów Nr 1 – Nr 5), wskazuje jej 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 podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami.

5. OŚWIADCZENIA:

1. Oświadczam(y), że moja oferta spełnia wszystkie wymagania i warunki ustalone w przedmiotowej Specyfikacji Istotnych Warunków Zamówienia,
2. Oświadczam(y), że wykonam zamówienie w terminie **90 dni** licząc od dnia podpisania umowy,
3. Oświadczam(y), że w cenie mojej oferty zostały uwzględnione wszystkie koszty niezbędne do prawidłowego wykonania zamówienia,
4. Oświadczam(y), że zapoznałem się ze SIWZ oraz projektem umowy i nie wnoszę do nich zastrzeżeń oraz przyjmuję warunki w nich zawarte,
5. Oświadczam(y), że uważam się za związanego złożoną ofertą na okres **60 dni** licząc od dnia otwarcia ofert,
6. Oświadczam(y), że akceptuję, iż zapłata za zrealizowanie zamówienia nastąpi w terminie do 30 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury,
7. Wadium do Pakietu Nr **……** w wysokości **…… PLN**, zostało wniesione

w dniu ..... **2017 roku**, w formie: ……,

8. Prosimy o zwrot wadium (wniesionego w pieniądzu), na zasadach określonych w art. 46 ustawy PZP, na następujący rachunek bankowy: ……,

6. ZOBOWIĄZANIA W PRZYPADKU PRZYZNANIA ZAMÓWIENIA:

1. Zobowiązujemy się do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego,
2. Osobą upoważnioną do kontaktów z Zamawiającym w sprawach dotyczących realizacji umowy jest ……, e-mail: ……, tel./fax: ……

7. PODWYKONAWCY:

Oświadczam(y), że przy realizacji zamówienia objętego przedmiotem niniejszego postępowania przetargowego **będę* / nie będę*** korzystać z usług podwykonawców.

* Niepotrzebne skreślić

W przypadku udziału podwykonawcy w realizacji zamówienia Zamawiający działając na podstawie art. 36b ust. 1 ustawy PZP żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, i podania przez wykonawcę (o ile są znani) firm podwykonawców:

1. ……,
2. ……,
3. ……,

8. TAJEMNICA PRZEDSIĘBIORSTWA:

Oświadczam(y), że niżej wymienione dokumenty składające się na ofertę zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i nie mogą być ogólnie udostępnione:

1. ……,
2. ……,
3. ……,

W celu wykazania, że powyżej wskazane dokumenty zawierają informacje stanowiące tajemnicę przedsiębiorstwa do oferty załączam:

1. ……,
2. ……,
3. ……,

9. SPIS TREŚCI:

Integralną część oferty stanowią następujące oświadczenia i dokumenty:

1. ……,
2. ……,
3. ……,
4. ……,
5. ……,
6. ……,
7. ……..

Oferta (wraz z załącznikami) została złożona na ..... **kolejno** ponumerowanych stronach.

10. OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI

Oświadczam, że wszystkie informacje podane w niniejszym formularzu oferty przetargowej oraz powyższe oświadczenia są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

…… Pieczęć Wykonawcy	…… Data i podpis upoważnionego przedstawiciela Wykonawcy

Załącznik Nr 2 do pisma z dnia 27 kwietnia 2017 roku – dot. pyt. i odp. do SIWZ – Nr 1
Załącznik Nr 6 do SIWZ
Opis Przedmiotu Zamówienia
Pakiet Nr 1 **Infrastruktura zwiększająca bezpieczeństwo sieci oraz infrastruktura serwerowa**

Szczegółowy opis przedmiotu zamówienia na zakup oprogramowania i sprzętu informatycznego: część 1 – Zwiększenie bezpieczeństwa sieciowego, dostawa sprzętu komputerowego oraz elementów infrastruktury serwerowej w ramach projektu „E-Usługi w informacji przestrzennej w Powiecie Tatrzańskim”.

I. Określenie przedmiotu zamówienia

Przedmiotem zamówienia jest **dostawa wraz z wdrożeniem infrastruktury zwiększającej bezpieczeństwo sieci oraz infrastruktury serwerowej dla Starostwa Powiatowego w Zakopanem**, w tym:

1) Dostawa, instalacja i konfiguracja infrastruktury zwiększających bezpieczeństwo sieci:
   a) Modernizacja sieci LAN (przełączniki 10 Gbps i 1Gbps) – 1 kpl.
   b) Modernizacja sieci WiFi (centralnie zarządzalne punkty WiFi) – 1 kpl.
   c) Zakup zestawu UTM (klaster) - ochrona styku Internet/Intranet – 1 kpl.
2) Dostawa, instalacja i konfiguracja zakresie infrastruktury serwerowej:
   a) Przełączniki rdzeniowe (switch) 10 G – 2 sztuki
3) Świadczenie usług gwarancyjnych i serwisowych wobec dostarczonego i zrealizowanego przedmiotu zamówienia

Terminy realizacji zamówienia:

Zakończenie realizacji całości zamówienia **w terminie do 90 dni od dnia podpisania umowy.**

Przeznaczenie realizowanego przedmiotu Zamówienia:

Niniejszy przedmiot zamówienia stanowi element dostawy infrastruktury zwiększającej bezpieczeństwo sieci w projekcie pn.: „E-Usługi w informacji przestrzennej w Powiecie Tatrzańskim", realizowanego w ramach Regionalnego Programu Operacyjnego Województwa Małopolskiego na lata 2014-2020, 2 Oś priorytetowa Cyfrowa Małopolska, Działanie 2.1 E-administracja i cyfrowe zasoby, Poddziałanie 2.1.4 e-Usługi w informacji przestrzennej.

W celu kompleksowego zwiększenia bezpieczeństwa przetwarzania i przesyłania danych w sieci

Internet/Intranet przedmiotem zamówienia stanowi zestaw UTM (klaster) z sygnaturami wraz z zintegrowanymi punktami dostępu WiFi, przełączniki sieciowe 10 Gbps i 1 Gbps.
Dostarczony przedmiot Zamówienia musi spełniać wymogi Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w zakresie dostarczonego oprogramowania.

II. Szczegółowy opis przedmiotu zamówienia:

1) Modernizacja sieci LAN (przełączniki 10 Gbps i 1Gbps) oraz przełączniki rdzeniowe (switch) 10 G

Podstawowe założenia

Podstawą realizowanego projektu „E-Usługi w informacji przestrzennej" będzie modernizacja sieci komputerowej LAN oraz dostawa przełączników rdzeniowych 10G w serwerowni.
Sieć LAN posłuży jako podstawowe medium komunikacyjne dla planowanych do wdrażania E-usług.
Przewiduje się, że modernizacja sieci LAN będzie zgodna z najnowszymi trendami i zasadami budowy wydajnych i bezpiecznych sieci komputerowych. Wykorzystane zostaną nowoczesne, ale już sprawdzone w wielu innych wdrożeniach mechanizmy.
Podstawowymi wymaganiami projektowymi będą:

- zgodność ze światowymi standardami transmisji danych,
- możliwość implementacji sieci wirtualnych i wirtualizację zasobów sprzętowych,
- gwarantowane duże pasmo przenoszenia (10Gb/s, łącza dostępowe 1Gb/s),
- możliwość implementacji zaawansowanych mechanizmów zapewnienia jakości transmisji (QoS),
- możliwość implementacji najnowszych rozwiązań zwiększających bezpieczeństwo w sieci takich jak 802.1x, Radius/TACACS+),
- zapewnienie wysokiej niezawodności i ciągłości działania sieci (odporność na awarie),
- zapewnienie ciągłości zasilania, wszystkie urządzenia infrastruktury informatycznej będą podtrzymywane przez zasilacze bezprzerwowe UPS,
- łatwość zwiększenia pasma w kierunku węzła centralnego (możliwość tworzenia łączy agregowanych),
- zapewnienie możliwości korzystania z bezprzewodowego dostępu do sieci w wybranych miejscach budynku urzędu,

Wymagania stawiane sieci LAN

Zgodnie z najlepszymi praktykami projektowania, topologia sieci LAN będzie hierarchiczna. W takiej architekturze wyróżnia się warstwy realizujące specyficzne funkcje, są to: dostępowa, dystrybucyjna, szkieletowa, serwerowa (rdzeniowa).

Warstwa szkieletowa ma za zadanie zapewnić bardzo wydajne połączenia dla ruchu przesyłanego między poszczególnymi węzłami sieci.
Warstwa dystrybucyjna ma za zadanie zapewnienie wydajnych połączeń pomiędzy przełącznikami w ramach jednego węzła sieci.
Warstwa dostępowa ma za zadanie zapewnić przyłącza dla użytkowników końcowych sieci korzystających z różnych stacji roboczych, desktopów, notebooków, terminali, itp.
Warstwa serwerowa (rdzeniowa) ma za zadanie zapewnić szybkie i niezawodne przyłącza dla farmy serwerów aplikacyjnych i bazodanowych.
Wszystkie urządzenia klienckie zostaną przyłączone do sieci przez urządzenia warstwy dostępowej - przełączniki sieciowe standardu 1Gb/10Gb. Przewiduje się zastosowanie przełączników posiadających 24/48 interfejsy 10/100/1000 (RJ-45) Ethernet (w tym 3 szt. przełączników w wersji z PoE), minimum cztery porty 10 Gigabit Ethernet w tym przynajmniej dwa porty zrealizowane w technologii światłowodowej (ze względu na oferowane przez taki port małe opóźnienia w serializacji pakietów) z przeznaczeniem na połączenia pomiędzy węzłami sieci oraz z przeznaczeniem na stack przełączników. Wymagana jest funkcja łączenia przełączników w stos.
Zakłada się, że przełączniki sieciowe będą miały skonfigurowane następujące mechanizmy związane z bezpieczeństwem: autoryzacja użytkowników/portów przez 802.1x.
Istotne jest też, aby porty dostępowe 10/100/1000 Ethernet (w przypadku przełączników w wersji z PoE) wspierały zasilanie urządzeń końcowych poprzez okablowanie strukturalne (Power over Ethernet) wg standardu IEEE 802.1at (30W per port). Funkcja ta umożliwi łatwe zasilanie urządzeń AP, itp.
Dla połączenia farmy serwerów do sieci zostanie przygotowana dedykowana warstwa urządzeń sieciowych – przełączniki 10G rdzeniowe przeznaczone do obsługi centralnych punktów sieciowych w serwerowni. Przewiduje się zastosowanie przełączników warstwy L3 posiadających minimum 24 interfejsy 10G. Planuje się uruchomienie jednego centrum przetwarzania danych w dwóch niezależnych lokalizacjach (serwerowni głównej oraz zapasowej) w celu maksymalizacji niezawodności realizowanych usług. Dla zapewnienia maksymalnej dostępności i bezpieczeństwa tych usług istotne będzie zaimplementowanie adekwatnych mechanizmów.

Ilość przełączników dostępowych jakie należy zastosować do modernizacji sieci LAN w punktach dystrybucyjnych przedstawia się następująco:
- serwerowni główna: 1 szt. 24 x 1Gb/s, 1 szt. 24 x 1Gb/s z POE
- punkt dystrybucyjny: 2 szt. 48 x 1 Gb/s, 1 szt. 48 x 1 Gb/s z POE
- serwerownia backup: 2 szt. 48 x 1 Gb/s, 1 szt. 24 x 1 Gb/s z POE

W serwerowni głównej planowane jest zastosowanie 2 szt. przełączników rdzeniowych minimum 24 porty x 10Gb/s przeznaczone do farmy serwerów.

Dostarczone przełączniki przez Wykonawcę należy wzajemnie skonfigurować tworząc stack w ramach punktów dystrybucyjnych. Połączenia pomiędzy przełącznikami muszą zapewniać najszybszą prędkość jakie przełączniki obsługują.

Wszystkie połączenia pomiędzy przełącznikami dystrybucyjnymi, punktami dystrybucyjnymi oraz przełącznikami szkieletowymi powinny mieć redundantne połączenia.
Pod potrzeby zasilania punktów dostępowych sieci bezprzewodowej należy zastosować przełącznik w technologii POE z tej samej serii co dostarczane przełączniki dostępowe tak aby można było przełączniki wzajemnie połączyć w stack w ramach punktów dystrybucyjnych.

System zarządzania przełącznikami

Zamawiający wymaga w ramach modernizacji sieci LAN dostawy, wdrożenia systemu zarządzającego dostarczonymi przełącznikami. System powinien:

- zapewniać zarządzanie min. 15 urządzeniami, musi być w pełni kompatybilny z dostarczanymi przełącznikami rdzeniowymi oraz dostępowymi
- zapewniać minimum obsługę 3 różnych typów producentów urządzeń sieciowych
- wspierać model architektury klient serwer oraz dostęp w oparciu o przeglądarkę
- zapewniać pojedynczy panel zarządzania zarówno dla sieci LAN
- zapewniać wyszukiwanie urządzeń sieciowych oraz prezentacje ich szczegółowych danych dotyczących ich funkcjonalności oraz szczegółów połączenia
- zapewniać prezentacje graficznej i fizycznej topologii map wszystkich zarządzanych urządzeń
- zapewniać grupowanie urządzeń w oparciu o model, lokalizacje, numer seryjny, MAC, FW i SW, itp.
- zapewniać dokonywania modyfikacji ustawień oraz oprogramowania dla wybranych wielu urządzeń jednocześnie
- zapewniać monitorowanie stanu i wydajności sieci oraz poszczególnych urządzeń
- zapewniać kreowanie tzw. Dashbord'ów zawierających informacje nt. zdarzeń sieciowych, wzorców ruchu sieciowego oraz trendów
- zapewniać proaktywne monitorowanie problemów sieciowych, automatyczne zmiany konfiguracyjne dla wielu urządzeń
- zapewniać gromadzenie danych dotyczących analizy przepływów sieciowych w oparciu o dedykowane protokoły sieciowe dla zapewnienia optymalizacji konfiguracji wydajności sieci
- zapewniać wsparcie dla autentykacji RADIUS, LDAP/AD

Schemat zakresu rekonfiguracji - modernizacji sieci LAN

1. Konfiguracja dostarczonych urządzeń, z uwzględnieniem:
   - Instancja sprzętu
   - Aktualizacja oprogramowania do najnowszej wersji
   - Wstępna konfiguracja sprzętu
   - Konfiguracja VLAN
   - Konfiguracja IP
   - Konfiguracja wszystkich połączeń w tym LACP
   - Konfiguracja protokołu Spanning Tree
   - Konfiguracja mechanizmów Quality of Service

2. Readresacja sieci LAN:
   - Zaprojektowanie nowego podziału adresacji sieci
   - Konfiguracja sieci VLAN
   - Konfiguracja polityk bezpieczeństwa pomiędzy poszczególnymi sieciami VLAN
   - Zmiana adresacji kluczowych elementów sieci
   - Rekonfiguracja serwerów DHCP
   - Aktualizacja rekordów DNS

3. Konfiguracja protokołu 802.1x
   - Konfiguracja polityk GPO - włączenie obsługi 802.1x na stacjach końcowych
   - Instalacja i konfiguracja usługi Radius na udostępnionym przez Zamawiającego posiadanych serwerze Windows 2012 Serwer R2 lub dostawa własnego oprogramowania przez Zamawiającego umożliwiającego implementację protokołu 802.1x
   - Instalacja serwera wydruku wraz z konfiguracją
   - Konfiguracja przełączników oraz urządzeń AP do współpracy z RADIUS'em
   - Konfiguracja VLAN
   - Konfiguracja polityk
   - Konfiguracja 802.1x
   - Konfiguracja bram w poszczególnych VLAN'ach
   - Konfiguracja list dostępowych ACL na bramach VLAN
   - Testy
   - Uruchomienie w środowisku produkcyjnym

4. Instalacja i konfiguracja oprogramowania do zarządzania przełącznikami.
   - Instalacja i konfiguracja oprogramowania w środowisku wirtualnym Zamawiającego
   - Założenie użytkowników i nadanie im odpowiednich uprawnień
   - Zeskanowanie nowego obszaru sieci, zaimportowanie urządzeń sieciowych do systemu oraz wykonanie mapy połączeń
   - Skonfigurowanie funkcjonalności systemu w zakresie realizacji wymagań stawianych systemowi zarządzania przełącznikami
   - Skonfigurowanie dla kilku przykładowych urządzeń: backup konfiguracji, odtwarzanie konfiguracji, zarządzanie awariami.

2) Modernizacja sieci WiFi (centralnie zarządzalne punkty WiFi)

Wymagania

Modernizowana sieć WiFi będzie spełniać następujące założenia:

- zapewnienie bezprzewodowego dostępu zgodnie ze standardami 802.11a/b/g/n/ac,
- system musi pracować w architekturze gwarantującej centralne zarządzanie infrastrukturą bezprzewodową z wykorzystaniem dostarczanego UTM,
- system musi zapewniać bezpieczną transmisję radiową zgodnie ze ogólnie obowiązującymi standardami

- system musi zapewniać realizację kontroli dostępu do medium bezprzewodowego (uwierzytelnianie, autoryzacja, rozliczenie użytkowników) przy wykorzystaniu zewnętrznych baz użytkowników typu np. RADIUS/AD,
- system musi zapewniać równoczesną obsługę zróżnicowanych zasad dostępu do medium bezprzewodowego
- system będzie wyposażony w mechanizmy przeciwdziałające zakłóceniom radiowym oraz przeciwdziałające zakłóceniom wywoływanym przez inne urządzenia WLAN (zaawansowane funkcje WIPS),
- przewiduje się zapewnienie zasięgu bezprzewodowego w budynku Starostwa w miejscach ustalonych na etapie projektu przed wykonawczego. Ze względu na wykorzystanie sprzętu komputerowego (przenośnego) w ramach projektu „E-Usługi w informacji przestrzennej w Powiecie Tatrzańskim" potrzeba jest zapewnienia dostępu do bezpiecznej sieci WiFi w określonych miejscach w urzędzie,
- przewiduje się zastosowanie 8 punktów dostępowych do sieci bezprzewodowej na sufitach pomieszczeń w wewnątrz budynku,
- okablowanie z zainstalowanych punktów dostępowych należy doprowadzić do najbliższych punktów dystrybucyjnych,
- system musi posiadać wydzielone zabezpieczone sieci, np. sieć administracyjna, sieć pracownicza, sieć gości – HotSpot,
- dla petentów urzędu powinna być wydzielona sieć bezprzewodowa z ograniczonym dostępem do Internetu - HotSpot. Petent nie powinien mieć dostępu do sieci lokalnej urzędu jedynie do sieci Internet oraz aby miał możliwość dostępu do planowanych E-Usług w ramach Geoportalu Powiatu Tatrzańskiego.

3) Zestaw UTM (klaster) - ochrona styku Internet/Intranet

Wymagania dotyczące instalacji i konfiguracji

Zestaw UTM musi być dostarczony w postaci dwóch fizycznych urządzeń (obydwa urządzenia muszą by tego samego modelu).

Do urządzeń musi być dostarczony niezbędny zestaw wyposażenia technicznego w tym np. kable, oraz licencja pozwalające na pracę dwóch urządzeń w trybie klastra HA (High Availability) typu active/active lub active/passive.

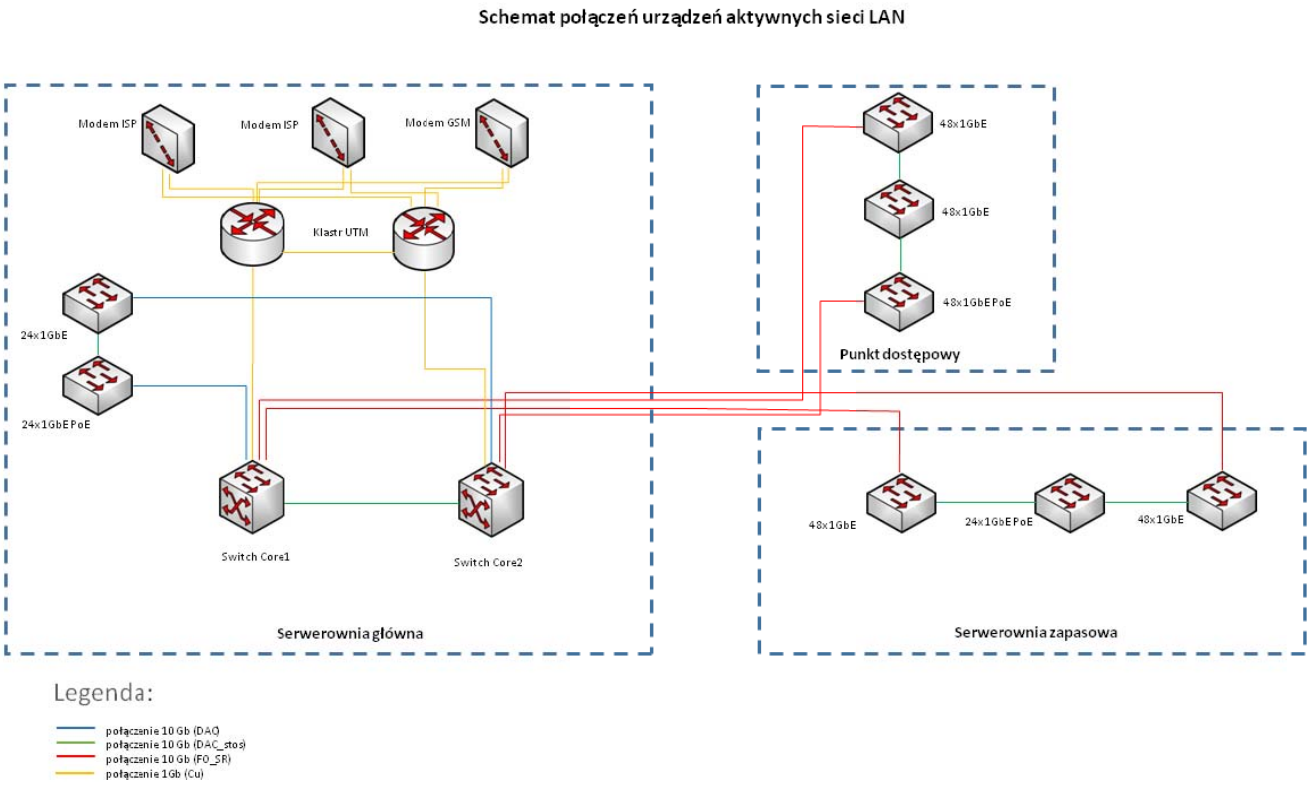
Instalacja i konfiguracja zestawu powinna uwzględniać montaż urządzeń w centrum przetwarzania danych. Zestaw powinien być skonfigurowany do pracy w trybie klastra z wykorzystaniem dwóch łączy internetowych (światłowodowych). Dodatkowo w celu skonfigurowania łącza zapasowego GSM, należy dostarczyć stosowny moduł GSM. Zamawiający posiada kartę SIM z aktywną usługą Internetu.

Schemat zakresu konfiguracji

- Inicjalna konfiguracja zestawu UTM (IP, hasła, NTP, DNS, licencje, użytkownicy),
- Utworzenie i konfiguracja klastra UTM,
- Konfiguracja wymaganych podsieci VLAN,

- Utworzenie polityk bezpieczeństwa zapewniających bezpieczeństwo przetwarzanych danych,
- Uruchomienie zaawansowanych funkcjonalności (np. w zakresie dostarczonych subskrypcji),
- Konfiguracja wymaganych połączeń tunelowych VPN,
- Uruchomienie serwera logów w systemie dołączonym do urządzenia,
- Uruchomienie i konfiguracja punktów dostępowych,
- Utworzenie i uruchomienie sieci WLAN działającej pod kontrolą UTM.

4) Schemat planowanej infrastruktury sieciowej oraz połączeń urządzeń aktywnych LAN



5) Świadczenie usług gwarancyjnych i serwisowych wobec całości dostarczonego i zrealizowanego przedmiotu zamówienia.

- Zamawiający wymaga, by Wykonawca udzielił na okres minimum 36 miesięcy gwarancji na dostarczone urządzenia lub na podstawie zapisu w wymiarze określonym dla każdego urządzenia.
- Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych poprzez serwis WWW lub faxem lub e-mailem lub telefonicznie w godzinach od 8-16 w dni robocze. Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań.
- W przypadku gdy awarii ulegnie dysk Wykonawca zobowiązany jest do wymiany na nowy a uszkodzony dysk pozostaje u Zamawiającego.
- W przypadku urządzeń, dla których jest wymagany dłuższy czas na usunięcie awarii, Zamawiający wymaga podstawienia na ten czas sprzętu zastępczego o nie gorszych

parametrach funkcjonalnych. Usunięcie awarii w takim przypadku nie może przekroczyć 15 dni roboczych od momentu zgłoszenia usterki.

- Przez cały okres trwania gwarancji:
  Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w godzinach pracy Zamawiającego w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych urządzeń.

Zamawiający uzyska dostęp do części chronionych stron internetowych producentów urządzeń, umożliwiający:

- pobieranie nowych wersji oprogramowania,
- dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
- dostęp do pomocy technicznej producentów.

III. Wymagania dotyczące realizacji przedmiotu zamówienia:

Projekt wdrożeniowy

W ramach realizacji zamówienia Wykonawca opracuje projekt wdrożeniowy przedmiotu zamówienia. Projekt wdrożenia musi być dostarczony Zamawiającemu do akceptacji przed przystąpieniem do dostawy, instalacji i konfiguracji przedmiotu zamówienia w wersji papierowej oraz w wersji elektronicznej umożliwiającej edycję.

Dostarczony projekt musi zawierać przynajmniej:

- Szczegółowy harmonogram wdrożenia, lista zadań do wykonania przez Wykonawcę i Zamawiającego.
- Procedurę instalacji i podłączenia urządzeń.
- Mapę topologii połączeń fizycznych i logicznych.
- Listę funkcjonalności i technologii planowanych do wdrożenia.
- Szablony konfiguracji urządzeń sieci LAN i bezprzewodowej uwzględniające: konfigurację VLAN, konfigurację zabezpieczeń i zarządzania, konfigurację interfejsów, konfigurację adresacji IP zgodnie z ustaleniami z Zamawiającym.
- Szablony konfiguracyjne urządzeń UTM uwzględniające: konfigurację zabezpieczeń i zarządzania, konfigurację redundancji urządzeń, konfigurację filtrowania ruchu.

Wdrożenie

Wykonawca dostarczy i skonfiguruje wszystkie elementy i podzespoły przedmiotu zamówienia do pełnej funkcjonalności wg przedłożonego Zamawiającemu i zaakceptowanego przez niego projektu wdrożeniowego umożliwiającego realizację funkcjonalności Projektu.

Wykonawca dostarczy komplet kabli, wkładek światłowodowych i innych elementów montażowych niezbędnych do uruchomienia wszystkich elementów dostarczanej konfiguracji i zainstalowania ich w szafach RACK 19'' Zamawiającego.

- Prace muszą być prowadzone w sposób niekolidujący z pracą urzędu, mając na uwadze szeroko rozumiany komfort petentów oraz pracowników.

- Formą akceptacji wszystkich prac będzie protokół odbioru, który będzie podpisywany pomiędzy Kierownikiem Projektu ze strony Wykonawcy i upoważnionym przedstawicielem Zamawiającego.
- **Wykonawca zgłosi pisemnie Zamawiającemu gotowość do odbioru wyników prac.**
- **Zamawiający rozpocznie weryfikację przekazanego przedmiotu zamówienia w terminie 7 dni roboczych od daty zgłoszenia gotowości odbioru.**
- W przypadku stwierdzenia przez Zamawiającego zastrzeżeń, wad, uwag bądź rozbieżności pomiędzy przekazanymi do weryfikacji wynikami danego etapu, a założeniami przyjętymi dla wykonania przedmiotu Umowy, Zamawiający sporządzi i przekaże Wykonawcy protokół rozbieżności.
- Po otrzymaniu protokołu rozbieżności, Wykonawca w terminie 7 dni roboczych lub innym wzajemnie uzgodnionym terminie dokona koniecznych poprawek, zmian lub udzieli wiążących wyjaśnień w tej sprawie i przekaże wyniki danego etapu do ponownej weryfikacji.
- Odbiór wykonanych prac uważa się za zakończony z chwilą podpisania bez zastrzeżeń odpowiedniego protokołu odbioru przez obie Strony, w ilości po jednym egzemplarzu dla każdej ze Stron
- **Ze względu na złożoność konfiguracji, Wykonawca ma zapewnić pracowników do realizacji projektu z kompetencjami potwierdzonymi certyfikatami w zakresie umiejętności konfiguracji sieci LAN oraz systemu UTM.**

Dokumentacja powykonawcza.

Przewiduje się wykonanie szczegółowego projektu wykonawczego dotyczącego z realizacji przedmiotu zamówienia. W szczególności dokument będzie zawierał:

- załączoną dokumentację producenta w zakresie konfiguracji dostarczonych elementów przedmiotu zamówienia
- opis funkcjonowania wysokiej dostępności usług sieci,
- listę testów akceptacyjnych systemu w szczególności weryfikujących poprawność działania mechanizmów realizujących wysoką dostępność usług sieci,
- nazewnictwo urządzeń, systemów, obiektów,
- opis sposobu współdziałania poszczególnych komponentów systemu,
- opis sposobu współdziałania dostarczonych elementów sieci LAN, WiFi, UTM z systemami sieci komputerowej, już istniejącymi u Zamawiającego,
- wytyczne dla realizacji przyjętej polityki bezpieczeństwa, wytyczne dla konfiguracji firewall'i,
- szczegółowe parametry konfiguracyjne dla poszczególnych komponentów systemu,
- ścieżki dostępu do panelów zarządczych, loginy i hasła administracyjne do urządzeń i oprogramowania stanowiący przedmiot zamówienia (jako oddzielny załącznik).

W ramach realizacji przedmiotu zamówienia Wykonawca przekaże dokumentację powykonawczą oraz zweryfikuje ją w obecności administratorów Zamawiającego ze stanem faktycznym realizowanego przedmiotu zamówienia. Dodatkowo w zakresie zwiększenia bezpieczeństwa

sieciowego Zamawiający otrzyma dokumentację certyfikowaną, voucher z zakresu Cobit Foundation oraz ITIL Foundation.

Wykonanie i dostarczenie dokumentacji powykonawczej jest warunkiem niezbędnym do rozpoczęcia przez Zamawiającego czynności odbiorowych gotowego systemu. Dokumentacja powykonawcza powinna być wykonana w formie elektronicznej i drukowanej w jednym egzemplarzu.

IV. Wymagania minimalne dla poszczególnych komponentów sprzętu i oprogramowania.

W poniższej specyfikacji wyszczególniono wymagane przez Zamawiającego parametry techniczne zamawianych elementów infrastruktury ICT. Od wykonawcy wymaga się także weryfikacji i traktowania wszystkich produktów jako powiązanych ze sobą i tworzących docelowy system informatyczny. Wykonawca zobowiązany jest również do zweryfikowania wszystkich aspektów polegających na wzajemnych powiązaniach systemu informatycznego z wszystkimi innymi systemami (np. weryfikacja warunków środowiskowych pracy urządzeń).

Modernizacja sieci LAN (przełączniki 10 Gbps i 1Gbps) – 1 kpl.		
Lp.	**Parametr**	**Minimalne wymagania**
1	2	3
1	Przeznaczenie	W ramach modernizacji sieci LAN należy wymienić przełączniki dystrybucyjne zastosowane w punktach dystrybucyjnych, łączące sieć strukturalną z zastosowaniem zabezpieczeń uwierzytelniania , tj. - serwerowni główna: 1 szt. 24 x 1Gb/s, 1 szt. 24 x 1Gb/s z PoE - punkt dystrybucyjny: 2 szt. 48 x 1 Gb/s, 1 szt. 48 x 1 Gb/s z PoE - serwerownia backup: 2 szt. 48 x 1 Gb/s, 1 szt. 24 x 1 Gb/s z PoE
2	Montaż	Urządzenie ma być zamontowane w szafie 19”. Wysokość nie większa niż 1U wersja RACK. Montaż z użyciem dedykowanych uchwytów.
3	Porty zainstalowane	Urządzenie powinno być wyposażone w następujące moduły: - Minimum 24 lub 48 porty GigabitEthernet w standardzie BaseT w zależności od wersji (24 x 1 Gb/s, 48 x 1Gb/s) - Wersja z PoE powinna obsługiwać przynajmniej połowę ilości portów przełącznika w standardzie PoE+ (tj. 12 /24 porty z PoE+) - minimum 4 porty 10Gb Ethernet w tym między innymi możliwość dedykowania dwóch portów 10Gb Ethernet SFP+ w celu połączenia przełączników w stos lub połączenia pomiędzy punktami dystrybucyjnymi - 1 port RJ45 umożliwiający zarządzanie poprzez konsolę
4	Stos	Urządzenie powinno posiadać możliwość łączenia w stos minimum 4 przełączników tego samego typu z PoE lub bez. Urządzenia dostarczone przez Wykonawcę powinny być połączone wzajemnie w stos przynajmniej na poziomie punktu dystrybucyjnego.
5	Wydajność	Urządzenie powinno posiadać następuje parametry minimalne: - Magistrala min.120 Gbps dla wersji 24 x 1 Gb/s lub min. 170 Gbps dla wersji 48 x 1 Gb/s - Prędkość przekazywanych pakietów: min. 95 Mpps dla wersji 24 x 1 Gb/s lub min. 130 Mbps dla wersji 48 x 1 Gb/s - Pamięć MAC adresów min. 16 000
6	Obsługa	TACACS+, RADIUS, ,Link aggregation, Wsparcie dla agregacji LACP (802.3ad)
7	Zarządzanie i bezpieczeństwo	Połączenie szyfrowane: SSL/SSH, Autentykacja dostępu do przełącznika w oparciu o Radius lub TACACS+ Listy dostępu (ACL) konfigurowalne dla fizycznego portu, łącza zagregowanego LAG i VLAN Obsługa SNMP v2 i v3, Możliwość przechowywania dwóch wersji oprogramowania na przełączniku, 802.1x w tm: - MAC-based authentication, - MAC authentication bypass, - Guest VLAN Zarządzenie przez CLI i przez przeglądarkę internetową **UWAGA – parametr służący wyłącznie ocenie ofert w kryterium wyboru oferty – Jakość**

		Obsługa standardu mierzenia przepływu sieciowego np. sFlow, NetFLow, IPFIX, : • Nie – 0 pkt, • Tak – 20 pkt.
8	Okablowanie	Wykonawca dostarczy komplet kabli połączeniowych w szczególności: kable statkujące - DAC, wkładki światłowodowe, krosowe światłowodowe oraz kable zasilające, itp.. Stackowanie przełączników jedynie przy użyciu kablami DAC lub światłowodowymi. Należy połączyć 3 punkty dystrybucyjne redundatnymi połączeniami SFP+ 10 Gb/s z przełącznikami rdzeniowymi w serwerowni głównej
9	Zasilanie:	1 zasilacz wbudowany
10	Gwarancja	Gwarancja min. 5 lat. W ramach gwarancji naprawa lub wymiana sprzętu na nowy. Czas reakcji serwisu w następnym dniu roboczym. Gwarancja obejmująca przełącznik oraz moduły i kable. W ramach gwarancji dostęp do nowych wersji oprogramowania. **UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Gwarancja** Wydłużenie okresu gwarancji przez okres posiadania sprzętu: • Gwarancja: 60 miesięcy – 0 pkt, • Gwarancja: dożywotnia – 15 pkt.
11	Certyfikaty	przełącznik musi posiadać deklaracja CE, został wyprodukowany zgodnie z normą ISO-9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność
12	Stan	Fabrycznie nowy

Przełącznik rdzeniowy (switch) 10G – 2 szt.		
Lp.	**Parametr**	**Minimalne wymagania**
1	2	3
1	Przeznaczenie:	Przełącznik zastosowany jako rdzeniowy łączący połączenia serwerów, macierzy oraz przełączników dystrybucyjnych.
2	Montaż:	Urządzenie musi mieć możliwość montażu w szafie 19”. Wysokość nie większa niż 1U wersja RACK. Montaż z użyciem dedykowanych uchwytów.
3	Porty zainstalowane:	Urządzenie powinno umożliwiać instalację następujących modułów: min. 24 x 10 GbE SFP+ w tym moduł min. 2 porty 40GbE QSFP+ umożliwiające zestackowanie przełączników.
4	Stos:	Urządzenie powinno zapewniać łączenie w stos minimum 4 przełączników. Urządzenia dostarczone przez Wykonawcę powinny być połączone wzajemnie w stos portami 40Gbe.
5	Wydajność:	Urządzenie powinno posiadać następuje parametry minimalne: Magistrala min. 600 Gbps; Prędkość przekazywanych pakietów: min. 450 Mpps. Pamięć MAC adresów min. 130 000
6	Obsługa:	Przełącznik warstwy 3 TACACS+, RADIUS, , Link aggregation, Wsparcie dla agregacji LACP (802.3ad)
7	Zarządzanie i bezpieczeństwo	Połączenie szyfrowane: SSL/SSH, Autentykacja dostępu do przełącznika w oparciu o Radius lub TACACS+ Listy dostępu (ACL) konfigurowalne dla fizycznego portu, łącza zagregowanego LAG i VLAN Obsługa SNMP v2 i v3, Obsługa sFlow, Możliwość przechowywania dwóch wersji oprogramowania na przełączniku, 802.1x w tm: - MAC-based authentication, - MAC authentication bypass, - Guest VLAN Zarządzenie przez CLI i przez przeglądarkę internetową, Port mirroring Liczniki pakietów wchodzących/wychodzących per każdy port Broadcast storm control
8	Okablowanie:	Wykonawca dostarczy kable przyłączeniowe do połączenia oferowanego urządzenia z dostarczanymi urządzeniami sieciowymi w szczególności: kable do statkowania kable krosowe

		światłowodowe wkładki światłowodowe oraz kable zasilające. Dodatkowo przełącznik powinien zapewniać podłączenie serwerów, np. powinien mięć zainstalowane przynajmniej wkładki 4 szt. 1 GbE T/przełącznik oraz 4 szt. 10 GbE SFP+ (dopuszcza się rozwiązanie połączenia za pomocą kabli DAC/TWINAX)/przełącznik.
9	Obudowa:	2 zasilacze redundantne wbudowane, redundantne wiatraki, chłodzenie przełącznika od portów Eth w kierunku zasilaczy (od przodu do tyłu urządzenia ze względu na strefy ciepła/zimna)
10	Gwarancja:	Min. 5 lat gwarancji obejmująca przełącznik oraz moduły i kable. W ramach gwarancji dostęp do nowych wersji oprogramowania. W ramach gwarancji naprawa lub wymiana sprzętu na nowy. Czas reakcji serwisu w następnym dniu roboczym.
11	Certyfikaty:	przełącznik musi posiadać deklaracja CE, został wyprodukowany zgodnie z normą ISO-9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność
12	Stan	Fabrycznie nowy

Modernizacja sieci WiFi (centralnie zarządzalne punkty WiFi) – 1 kpl.		
Lp.	**Parametr**	**Minimalne wymagania**
1	2	3
1	Przeznaczenie	Modernizacja obecnie użytkowanych punktów dostępowych oraz dołożenie nowych w wymaganych do pokrycia zasięgiem sygnału WiFi obszaru na którym będą użytkowane urządzenia mobilne.
2	Montaż	8 sztuk punktów WiFi należy zamontować we wskazanych miejscach przez Zamawiającego do sufitu pomieszczeń budynku. Należy doprowadzić okablowanie z punktów dystrybucyjnych do niniejszych punktów WiFi.
3	Kontroler	Urządzenia zarządzane i zintegrowane na poziomie dostarczanego UTM. Zarządzanie z GUI wspólnego z UTM.
4	Prędkość	Maksymalna powyżej 1 Gbps
5	Parametry fizyczne	1 x 1000BASE-T IEEE 802.3af/at Obsługa technologii 802.11n i praca w technice transmisji wieloantenowej MIMO 3x3
6	Wspierane protokoły i funkcje	802.11a/b/g/n/ac, 802.11i, 802.1q, 802.1X, 802.3af/at, 802.11e, 2.4 oraz 5 GHz
7	Dodatkowe:	Wraz z punktem dostępowym należy dostarczyć dedykowany uchwyt umożliwiający montaż punktu dostępowego pod sufitem.
8	Gwarancja:	Min. 3 lata gwarancji. W ramach gwarancji dostęp do nowych wersji oprogramowania. W ramach gwarancji naprawa lub wymiana sprzętu na nowy. Czas reakcji serwisu w ciągu 3 dni roboczych. **UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Gwarancja** Wydłużenie okresu gwarancji: • Gwarancja: 36 miesięcy – 0 pkt, • Gwarancja: 37 – 44 miesięcy – 1 pkt, • Gwarancja: 45 – 50 miesięcy – 2 pkt, • Gwarancja: 51 – 55 miesięcy – 3 pkt, • Gwarancja: 56 – 59 miesięcy – 4 pkt, • Gwarancja: 60 miesięcy – 5 pkt,
9	Certyfikaty:	Urządzenie musi posiadać certyfikat CE, został wyprodukowany zgodnie z normą ISO-9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność
10	Stan	Fabrycznie nowy

Zakup zestawu UTM (klaster) - ochrona styku Internet/Intranet		
Lp.	**Parametr**	**Minimalne wymagania**
1	2	3
1	Architektura	System musi być dostarczony w postaci dwóch fizycznych urządzeń (obydwa urządzenia muszą by tego samego modelu). Do urządzeń musi być dostarczony niezbędny zestaw wyposażenia technicznego w tym np. kable, oraz licencje pozwalające na pracę dwóch urządzeń w trybie klastra HA (High Availability) typu active/active lub active/passive
2	Funkcjonalności rozwiązania	Musi wspierać trzy strefy bezpieczeństwa (DMZ) Musi wspiera statyczne i dynamiczne adresy IP (DHCP i PPoE) na zewnętrznym interfejsie Przepustowość Firewall: Musi obsługiwać przepustowość UTM min. 500 Mbps Musi obsługiwać min. 1 700 000 jednoczesnych połączeń Urządzenie musi posiadać cechy zabezpieczenia UTM, włącznie z filtrowaniem zawartości URL, IPS, GAV, kontroli aplikacji, DLP, oraz ochroną przed zagrożeniami typu zero-day Musi posiadać wsparcie dla implementacji polityki bezpieczeństwa w warstwie aplikacji jako proxy aplikacji. Rozwiązanie musi zawierać zasady bezpieczeństwa proxy w warstwie aplikacji, skonfigurowane domyślnie do wspierania następujących wspólnych protokołów: HTTP, HTTPs, POP3, SMTP, FTP, DNS, SIP, H323 Urządzenie musi wspierać uwierzytelnianie poprzez RADIUS, SecureID, LDAP i Active Directory. Musi obsługiwać uwierzytelnianie serwerów Active Directory w trybie transparent (Single-Sign-On). W urządzeniu nie powinno być żadnych ograniczeń liczby użytkowników pracujących online. Musi posiadać wsparcie Dynamic DNS. Rozwiązanie musi posiadać obronę przeciwko pofragmentowanym atakom, dzięki czemu będzie w stanie zmontować pofragmentowane pakiety przed przekazaniem ich do sieci wewnętrznej. Urządzenie musi mieć funkcjonalność pozwalającą na filtrowanie treści najpopularniejszych protokołów, jak i również na filtrowanie według typu MIME Musi mieć możliwość chronienia wewnętrznych serwerów pocztowych przeciwko atakom typu spam z możliwością konfiguracji komputera dla domen akceptujących e-mail. Musi posiadać możliwość konfiguracji progów bezpieczeństwa dla wykrywania ataków typu flood, DoS, oraz DDoS Firewall musi wspierać protokół wykrywania anomalii w DNS i w innych popularnych protokołach.
3	VPN	Musi posiadać wsparcie dla mobilnych sieci VPN Musi obsługiwać co najmniej 20 mobilnych połączeń VPN IPSec Musi obsługiwać co najmniej 20 mobilnych połączeń VPN SSL Musi posiadać możliwość pobrania klienta SSL bezpośrednio z urządzenia Niezbędna jest dostępność klienta SSL dla przynajmniej dla systemów operacyjnych posiadanych przez Zamawiającego: Windows Vista, Windows 7, 8, 10 jak i również dla Android Musi posiadać wsparcie dla VPN pomiędzy oddziałami Musi obsługiwać co najmniej 5 połączeń VPN między oddziałami poprzez IPSec Urządzenie musi być w stanie współdziałać z produktami innych marek, które wspierają obsługę IPSec Rozwiązanie musi wspierać mechanizmy uwierzytelniania DES, 3DES, AES 128 -, 192 -, 256-bit Rozwiązanie musi wspierać mechanizmy szyfrowania SHA-1, SHA-2,MD5, IKE Pre-Shared Key, 3rd Party Cert. Musi posiadać wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego) Musi posiadać przepustowość IPSec VPN nie mniejsza niż 1200 Mbps Musi mieć możliwość tworzenia wirtualnych interfejsów VPN site-site oraz VPN poprzez Dynamic Routing Protocols

4	Filtrowanie zawartości URL i kontrola aplikacji	Możliwość wspierania filtrowania zawartości w urządzeniu poprzez stosowanie subskrypcji Funkcjonalność filtrowania zawartości powinna zawierać możliwość filtrowania użytkowników lub grup użytkowników Rozwiązanie powinno pozwalać na tworzenie białych list wyjątków dla filtrowania zawartości Baza zawartości URL powinna być dynamicznie aktualizowana Funkcja powinna filtrować treści w wielu językach, w tym w języku polskim Urządzenie powinno identyfikować i blokować wiele różnych aplikacji, w tym mieć możliwość szczegółowej kontroli funkcji i aplikacji, takich jak logowanie i transfer plików Niezbędna jest automatyczna i regularna aktualizacja sygnatur aplikacji
5	Antywirus	Musi posiadać możliwość wsparcia systemu antywirusowego z poziomu urządzenia poprzez subskrypcje Musi posiadać automatyczną aktualizację plików sygnatur antywirusowych Antywirus musi mieć możliwość przeprowadzania kwarantanny e-mail. Rozwiązanie musi mieć możliwość tworzenia wyjątków w białej liście, aby umożliwić nieblokowany dostęp do poczty z określonych domen Musi posiadać blokowanie spyware Musi posiadać skanowanie wszystkich plików skompresowanych (np.: zip, tar, rar, gzip) z wieloma poziomami kompresji Musi posiadać wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3 Musi posiadać możliwość funkcjonalności opartej na chmurze pozwalającej na wprowadzenie oceny reputacji Usługa musi być w stanie zablokować strony internetowe ze złą reputacją bazując na informacjach pobranych z chmury (historia wirusów, smapu i innych rodzajów złośliwego oprogramowania) Musi posiadać przepustowość AV w urządzeniu nie mniejsza niż 600 Mbps
6	Antyspam	Możliwość wsparcia systemu antyspamowego z poziomu urządzenia poprzez subskrypcje Antyspam musi zapewnić możliwość kwarantanny e-mail Antyspam musi posiadać zintegrowaną antywirusową analizę spamu Rozwiązanie musi umożliwić blokowanie spamu w wielu językach w tym w języku polskim Musi posiadać możliwość blokowania spamu opartego na obrazach graficznych (OCR).
7	IPS	Musi posiadać możliwość wsparcia IPS z poziomu urządzenia poprzez subskrypcje Musi posiadać automatyczną aktualizacja sygnatur IPS IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy Musi posiadać automatyczne blokowanie znanych źródeł ataków Musi posiadać wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3 Musi posiadać przepustowość IPS w urządzeniu nie mniejszą niż 1 Gbps
8	NAT	Urządzenie musi wpierać NAT i PAT. Musi posiadać wspieranie równoważenia obciążenia serwerów dla urządzeń wewnętrznych Musi posiadać wsparcie dla Static NAT (Port Forwarding) Musi posiadać wsparcie dla Dynamic NAT Musi posiadać wsparcie dla NAT One-to-One Musi posiadać wsparcie dla IPSec NAT Traversal Musi posiadać wsparcie dla policy-based NAT
9	Parametry sieciowe	Ilość interfejsów sieciowych: minimum 8x 10/100/1000 BaseT interface. Interfejsy te powinny być skonfigurowane jako jeden z trzech rodzajów wymaganych stref bezpieczeństwa Wsparcie Multi-WAN. Urządzenie musi obsługiwać co najmniej trzy zewnętrzne źródła połączenia z Internetem. Interfejsy te muszą umożliwiać działanie w trybie fail-over Interfejsy zewnętrzne muszą również działać w trybie „round-robin” Interfejsy zewnętrzne muszą również działać jako „overflow" Wsparcie VLAN: musi posiadać minimum 10 sieci VLAN Urządzenie musi także zapewniać kontrolę ruchu dla użytkowników, polityk, protokołu, grupy użytkowników. Musi zapewnić kontrolę ruchu dla wszystkich interfejsów. Musi zapewnić kontrolę ruchu adresu IP oraz sieci VLAN

		Musi zapewnić kontrolę ruchu aplikacji i kategorii aplikacji Rozwiązanie musi wspierać implementację w trybie routera (routing), tryb drop-in (ten sam adres IP na wszystkich interfejsach), oraz w trybie transparent-bridge Powinno musi wspierać statyczny i dynamiczny NAT, oraz 1-1 NAT Rozwiązanie musi pracować w trybie HA Musi posiadać wsparcie dla routingu opartego na regułach (Policy Based Routing)
10	Zarządzenie	Administracja urządzenia musi być możliwe poprzez graficzny interfejs zarządzania w czasie rzeczywistym. Musi zapewniać monitorowanie logów ruchu w czasie rzeczywistym. Rozwiązanie musi zapewniać wysyłanie alarmów przez SNMP lub e-mail. Musi posiadać wsparcie zarządzania protokołami DVCP (Dynamic VPN Control Protocol) Musi posiadać obsługę różnych ról administratorów. Użytkownicy muszą być uwierzytelnieni przez zewnętrzny serwer z użytkownikami. Urządzenie musi wspierać zarządzanie przez przeglądarkę WWW. Urządzenie musi zapewniać zarządzanie za pomocą linii poleceń poprzez port szeregowy lub poprzez SSH. Interfejs WWW do zarządzania urządzeniem musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach mobilnych typu tablet lub smartfon. System musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia, bez konieczności podłączenia się do niego.
11	Dzienniki i raporty	Oferowane rozwiązanie musi umożliwić stosowanie serwerów zewnętrznych w drodze do scentralizowania przechowywania dzienników i raportów. Niedopuszczalne jest stosowanie dodatkowych opłat za rozwiązanie do rejestrowania i raportowania Usługa musi być oparta na TCP oraz korzystać z bazy danych SQL, aby zapewnić jej pełną skalowalność. Powinno być możliwe zdefiniowanie wielu serwerów dziennika. Urządzenie musi mieć możliwość współpracy z dwoma serwerami dzienników, jednego głównego, oraz drugiego w przypadku awarii. Dzienniki transmisji muszą być odpowiednio szyfrowane. Rozwiązanie musi posiadać ponad 50 predefiniowanych typów raportów, bez żadnych dodatkowych opłat i kosztów. Urządzenie musi mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV. System musi być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania tych sprawozdań pocztą e-mail. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości. System raportowania powinien być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów i dzienników. Narzędzie do tworzenia dzienników i raportów musi wspierać posiadaną przez Zamawiającego platformę Vmware. System musi zapewniać wizualizację, opisującą w trybie graficznym stan przepustowości systemu. System musi mieć możliwość przedstawienia na mapie świata źródła i celów zagrożeń, ruchu aplikacji, blokowania dostępu oraz wydarzeń IPS. Raporty IPS muszą prowadzić do portalu internetowego dostarczającego szczegółowe informacje dotyczącego każdego zdarzenia. Możliwość grupowania urządzeń, w celu tworzenia raportów sumarycznych.
12	Blokowanie APT	Musi posiadać możliwość wsparcia blokowania dla nieznanego złośliwego oprogramowania z poziomu urządzenia poprzez subskrypcje
13	Oprogramowanie monitorujące (sensory)	Musi posiadać w zestawie możliwość instalacji sensorów na stacjach klienckich w celu wykrywania stanu bezpieczeństwa stacji. Wymagana dostawa subskrypcji
14	Gwarancja	Urządzenia muszą być dostarczone z min. 3 letnią gwarancja, świadczoną w następnym dniu

		roboczym, oraz z bezpłatną subskrypcją aktualizacji oprogramowania oraz definicji sygnatur w okresie obowiązywania gwarancji.
15	Certyfikaty:	Urządzenie musi posiadać certyfikat CE, został wyprodukowany zgodnie z normą ISO-9001 lub równoważny certyfikat wydany przez inne jednostki oceniające zgodność
16	Stan	Fabrycznie nowy

Załącznik Nr 3 do pisma z dnia 27 kwietnia 2017 roku – dot. pyt. i odp. do SIWZ – Nr 1
Załącznik Nr 7 do SIWZ
Opis Przedmiotu Zamówienia
Pakiet Nr 2 **Oprogramowanie zwiększające bezpieczeństwo sieci**

Szczegółowy opis przedmiotu zamówienia na zakup oprogramowania i sprzętu informatycznego: część 1 – Zwiększenie bezpieczeństwa sieciowego, dostawa sprzętu komputerowego oraz elementów infrastruktury serwerowej w ramach projektu „E-Usługi w informacji przestrzennej w Powiecie Tatrzańskim”.

I. Określenie przedmiotu zamówienia

Przedmiotem zamówienia jest **dostawa wraz z wdrożeniem oprogramowania zwiększające bezpieczeństwo sieci dla Starostwa Powiatowego w Zakopanem**, w tym:

1) Dostawa, instalacja i konfiguracja pakietu oprogramowania monitorowania bezpieczeństwa IT – 1 szt.
2) Dostawa pakietu oprogramowania antywirusowego – 1 szt.
3) Dostawa certyfikatów kwalifikowanych dla Wydziału Geodezji, Kartografii, Katastru i Gospodarki Nieruchomości – 5 szt.
4) Świadczenie usług gwarancyjnych wobec dostarczonego i zrealizowanego przedmiotu zamówienia

Terminy realizacji zamówienia:

Zakończenie realizacji całości zamówienia **w terminie do 90 dni od dnia podpisania umowy.**

Przeznaczenie realizowanego przedmiotu Zamówienia:

Niniejszy przedmiot zamówienia stanowi element dostawy oprogramowania zwiększającego bezpieczeństwo sieci w projekcie pn.: „E-Usługi w informacji przestrzennej w Powiecie Tatrzańskim", realizowanego w ramach Regionalnego Programu Operacyjnego Województwa Małopolskiego na lata 2014-2020, 2 Oś priorytetowa Cyfrowa Małopolska, Działanie 2.1 E-administracja i cyfrowe zasoby, Poddziałanie 2.1.4 e-Usługi w informacji przestrzennej.
W celu kompleksowego zwiększenia bezpieczeństwa przetwarzania i przesyłania danych w sieci Internet/Intranet przedmiotem zamówienia stanowi pakiet oprogramowania monitorowania

bezpieczeństwa IT, licencja pakietu oprogramowania antywirusowego, certyfikaty kwalifikowane dla wskazanych pracowników Wydziału Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami.

Dostarczony przedmiot Zamówienia musi spełniać wymogi Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w zakresie dostarczonego oprogramowania.

II. Wymagania dotyczące realizacji przedmiotu zamówienia:

Projekt wdrożeniowy

W ramach realizacji zamówienia Wykonawca opracuje projekt wdrożeniowy przedmiotu zamówienia. Projekt wdrożenia musi być dostarczony Zamawiającemu do akceptacji przed przystąpieniem do dostawy, instalacji i konfiguracji przedmiotu zamówienia w wersji papierowej oraz w wersji elektronicznej umożliwiającej edycję.

Dostarczony projekt musi zawierać przynajmniej:

- Szczegółowy harmonogram wdrożenia, lista zadań do wykonania przez Wykonawcę i Zamawiającego
- Niezbędne wymagania w zakresie zasobów sprzętowych umożliwiających przeprowadzenie procedury instalacji
- Procedurę instalacji oraz konfiguracji oprogramowania.
- Listę funkcjonalności i technologii planowanych do wdrożenia
- Szablony uprawnień dla administratorów i operatorów oprogramowania w zakresie zwiększenia bezpieczeństwa sieci

Wdrożenie.

Wykonawca dostarczy i skonfiguruje wszystkie elementy przedmiotu zamówienia do pełnej funkcjonalności wg przedłożonego Zamawiającemu i zaakceptowanego przez niego projektu wdrożeniowego umożliwiającego realizację funkcjonalności Projektu.

- Prace muszą być prowadzone w sposób niekolidujący z pracą urzędu, mając na uwadze szeroko rozumiany komfort petentów oraz pracowników.
- Formą akceptacji wszystkich prac będzie protokół odbioru, który będzie podpisywany pomiędzy Kierownikiem Projektu ze strony Wykonawcy i upoważnionym przedstawicielem Zamawiającego.
- **Wykonawca zgłosi pisemnie Zamawiającemu gotowość do odbioru wyników prac.**
- **Zamawiający rozpocznie weryfikację przekazanego przedmiotu zamówienia w terminie 7 dni roboczych od daty zgłoszenia gotowości odbioru.**
- W przypadku stwierdzenia przez Zamawiającego zastrzeżeń, wad, uwag bądź rozbieżności pomiędzy przekazanymi do weryfikacji wynikami danego etapu, a założeniami przyjętymi

dla wykonania przedmiotu Umowy, Zamawiający sporządzi i przekaże Wykonawcy protokół rozbieżności.

- Po otrzymaniu protokołu rozbieżności, Wykonawca w terminie 7 dni roboczych lub innym wzajemnie uzgodnionym terminie dokona koniecznych poprawek, zmian lub udzieli wiążących wyjaśnień w tej sprawie i przekaże wyniki danego etapu do ponownej weryfikacji.
- Odbiór wykonanych prac uważa się za zakończony z chwilą podpisania bez zastrzeżeń odpowiedniego protokołu odbioru przez obie Strony, w ilości po jednym egzemplarzu dla każdej ze Stron
- Wykonawca ma zapewnić pracowników do realizacji projektu posiadających niezbędną wiedzę do należytego wdrożenia pakietu oprogramowania.

Dokumentacja powykonawcza.

Przewiduje się wykonanie szczegółowego projektu wykonawczego dotyczącego z realizacji przedmiotu zamówienia. W szczególności dokument będzie zawierał:

- załączoną dokumentację producenta w zakresie konfiguracji dostarczonych elementów przedmiotu zamówienia
- opis funkcjonalności wdrożonego przedmiotu zamówienia,
- szczegółowe parametry konfiguracyjne dla poszczególnych komponentów systemu.
- listę testów akceptacyjnych systemu w szczególności weryfikujących poprawność działania mechanizmów realizujących wdrożone funkcjonalności,
- nazewnictwo urządzeń, systemów, obiektów,
- opis sposobu współdziałania poszczególnych komponentów systemu,
- opis sposobu współdziałania dostarczonych elementów oprogramowania z systemami ICT już istniejącymi u Zamawiającego,
- wytyczne dla realizacji przyjętej polityki bezpieczeństwa,
- ścieżki dostępu do panelów zarządczych, loginy i hasła administracyjne do urządzeń i oprogramowania stanowiący przedmiot zamówienia (jako oddzielny załącznik).

W ramach realizacji przedmiotu zamówienia Wykonawca przekaże dokumentację powykonawczą oraz zweryfikuje ją w obecności administratorów Zamawiającego ze stanem faktycznym realizowanego przedmiotu zamówienia. Dodatkowo w zakresie zwiększenia bezpieczeństwa sieciowego Zamawiający otrzyma dokumentację certyfikowaną, voucher z zakresu Cobit Foundation oraz ITIL Foundation.

Wykonanie i dostarczenie dokumentacji powykonawczej jest warunkiem niezbędnym do rozpoczęcia przez Zamawiającego czynności odbiorowych gotowego systemu. Dokumentacja powykonawcza powinna być wykonana w formie elektronicznej i drukowanej w jednym egzemplarzu.

Świadczenie usług gwarancyjnych wobec dostarczonego i zrealizowanego przedmiotu zamówienia.

Zamawiający wymaga, by Wykonawca udzielił na okres jednego roku gwarancji na dostarczone oprogramowanie lub na podstawie zapisu w wymiarze określonym dla każdego oprogramowania / modułu.

Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych poprzez serwis WWW lub faxem lub e-mailem lub telefonicznie w godzinach od 8-16 w dni robocze. Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań.

Przez cały okres trwania gwarancji:

1. Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w godzinach pracy Zamawiającego w zakresie rozwiązywania awarii i błędów uniemożliwiających bieżącej eksploatacji dostarczonego oprogramowania.
2. Zamawiający uzyska dostęp do części chronionych stron internetowych producentów oprogramowania, umożliwiający:
   - pobieranie nowych wersji oprogramowania,
   - dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
   - dostęp do pomocy technicznej producentów.

III. Wymagania minimalne dla poszczególnych komponentów sprzętu i oprogramowania.

W poniższej specyfikacji wyszczególniono wymagane przez Zamawiającego parametry techniczne zamawianego oprogramowania ICT. Od wykonawcy wymaga się także weryfikacji i traktowania wszystkich produktów jako powiązanych ze sobą i tworzących docelowy system informatyczny.

Pakietu oprogramowania monitorowania bezpieczeństwa IT		
Lp.	**Parametr**	**Minimalne wymagania**
1	2	3
1	Przeznaczenie	Pakiet oprogramowania monitorowania bezpieczeństwa IT będzie dotyczył bezpieczeństwa teleinformatycznego w dwóch głównych obszarach: - monitorowanie sieci oraz zarządzanie zdarzeniami i logami - monitorowanie i zarządzaniem sprzętem komputerowym oraz użytkownikami W związku ze stale rosnącymi zagrożeniami wymaga się dostawy pakietu oprogramowania monitorowania IT obejmujący funkcjonalności niezbędne do podniesienia bezpieczeństwa teleinformatycznego: wykrywanie i skanowanie sieci, stałe monitorowanie zagrożeń, zbieranie i zarządzanie logami oraz korelacja zdarzeń, audyt zasobów sprzętowych i oprogramowania, monitorowanie aktywności użytkowników, pomoc użytkownikom sieci, kontrola dostępu użytkowników do urządzeń i nośników danych oraz alarmowanie i raportowanie
2	Licencja	Licencja na pakiet oprogramowania jest bezterminowa. Musi zostać zapewnione minimum 1 roczny okres aktualizacji oprogramowania, subskrypcji oraz wsparcie producenta. Pakiet oprogramowania powinien zapewniać dostęp do konsoli zarządczej przynajmniej trzem administratorom. Dopuszcza się zaoferowanie dwóch licencji programów w pakiecie (ze względu na nieograniczanie konkurencji) obsługujących poszczególne obszary bezpieczeństwa pakietu oprogramowania. **UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Subskrypcja** Wydłużenie okresu aktualizacji oprogramowania, subskrypcji zagrożeń dotyczących obszaru monitorowania sieci oraz zarządzania zdarzeniami i logami: • Subskrypcja: 12 miesięcy – 0 pkt, • Subskrypcja: 13 – 15 miesięcy – 5 pkt. • Subskrypcja: 16 – 18 miesięcy – 10 pkt. • Subskrypcja: 19 – 21 miesięcy – 15 pkt. • Subskrypcja: 22 – 23 miesięcy – 20 pkt. • Subskrypcja: 24 miesiące – 30 pkt.
3	Monitorowanie sieci oraz zarządzanie zdarzeniami i logami	Rozwiązanie musi umożliwiać wdrożenie pełnej wymaganej funkcjonalności na platformie wirtualizacyjnej. Rozwiązanie musi być zdolne do identyfikacji ruchu sieciowego w sieciach środowisk wirtualnych. System musi zapewniać możliwość zbierania logów z co najmniej 25 źródeł Rozwiązanie powinno posiadać wsparcie producenta, ale też wsparcie w formie dostępnego forum wymiany wiedzy/doświadczeń dotyczące produktu, które zostanie udostępnione bez limitu operatorom i administratorom systemu. Rozwiązanie musi wspierać długoterminowe zapewnienie dostępu do szczegółowych danych odnośnie zarejestrowanych i zebranych zdarzeń czy przepływów w sieci. System powinien zapewnić dostęp do takich informacje co najmniej przez okres trwania subskrypcji. Licencja powinny być bezterminowe i nie uzależnione od wykupienia lub przedłużenia wsparcia producenta.
		W zakresie monitorowania sieci oraz zarządzanie zdarzeniami i logami musi zapewnić: Wykrywanie i skanowanie sieci Stałe monitorowanie zagrożeń Zbieranie i zarządzanie logami Korelacja zdarzeń
		Rozwiązanie musi zapewnić możliwość uchwycenia i prezentacji wszystkich istotnych aspektów

		incydentu bezpieczeństwa w jednym logicznym widoku. Widok taki powinien zawierać minimalnie informacje typu: powiązane zdarzenia, aktywność sieciowa, skorelowane alerty, skorelowane podatności w powiązanych systemach, itp.
		Rozwiązanie musi umożliwiać szyfrowanie komunikacji pomiędzy poszczególnymi modułami systemu i zbierania danych. Rozwiązanie musi umożliwiać integrację z zewnętrznymi dostawcami mechanizmów uwierzytelniania (LDAP, AD, RADIUS, etc...) dla operatorów i administratorów systemu
		Rozwiązanie musi wspierać informacje NetFlow - czyli dane o przepływach, np.: NetFlow, J- Flow, sFlow, IPFIX, itp.
		Wykrywanie i rejestrowanie dla celów audytowych zmian w konfiguracji urządzeń sieciowych, zawiadamianie użytkowników o działaniu niezgodnym ze zdefiniowanymi politykami (zasadami). Możliwość analizy na poziomie sieciowym, kto był zaangażowany w incydent, co się stało, kiedy zaszło zdarzenie, jakie dane zostały udostępnione lub przekazane.
		Rozwiązanie musi posiadać mechanizmy usprawniające jego wykorzystanie i wdrożenie, np.: - automatyczne wykrywanie źródeł logów - automatyczne wykrywanie aplikacji - automatyczne wykrywanie aktywów - automatyczne wykrywanie podatności - automatyczne wykrywanie anomalii - automatyczne grupowanie aktywów - predefiniowane reguły analizy i korelacji zdarzeń - łatwe w użyciu mechanizmy filtrowania (również predefiniowane filtry) - zaawansowane funkcje analizy zabezpieczeń - predefiniowane raporty - priorytetyzacja wg zasobów - automatyczne aktualizacje baz zagrożeń, wsparcia urządzeń, oprogramowania systemowego,
		Rozwiązanie musi zapewniać ciągłe działanie jak największej liczby komponentów, niezależnie od awarii jednego z nich. Np. w sytuacji awarii systemu centralnego lub modułu analitycznego, logi powinny być nadal zbierane. Rozwiązanie musi posiadać mechanizmy umożliwiające zbieranie danych w czasie rzeczywistym.
		Rozwiązanie powinno posiadać pewną ilość przykładowych skonfigurowanych paneli (dashboards), prezentujących możliwości i mechanizmy systemu.
		Rozwiązanie musi utrzymywać bazę wiedzy o wszystkich wykrytych w sieci aktywach. Wśród zgromadzonych danych o danym aktywie powinny być zawarte pewne informacje uzyskane przy wykrywaniu zasobów: - atrybuty systemu - atrybuty sieciowe - stan - podatności/luki - lokalizacja - przynależność - inne właściwości, które użytkownik może samodzielnie zdefiniować i/lub wpisywać.
		Rozwiązanie musi wspierać informacje zbierane z systemów operacyjnych w wersji serwerowej. Rozwiązanie musi wspierać informacje zebrane z infrastruktury sieciowej (switche, routery, itp.). Rozwiązanie musi posiadać własny skaner podatności.
		Rozwiązanie musi zapewniać możliwość przechowywania zarówno znormalizowanych danych o zdarzeniach, jak również źródłowego/oryginalnego formatu danych w tzw. postaci RAW, np. dla celów późniejszej analizy w innych systemach lub przeprowadzenia analizy śledczej.
		Rozwiązanie musi posiadać architekturę pozwalającą na zbieranie i archiwizację logów, w podziale na dane krótkoterminowe (tzw. online, wykorzystywane w bieżących analizach) oraz dane długoterminowe (tzw. offline, dane archiwizowane po określonym czasie), z wewnętrzną ale konfigurowalną obsługą mechanizmu retencji danych pomiędzy obydwoma typami. Rozwiązanie powinno wspierać przechowywanie (archiwizację) logów na zewnętrznych urządzeniach do składowania danych. Rozwiązanie musi wspierać mechanizmy zbierania logów (np.: syslog, WMI, JDBC, SNMP, itp.). System powinien wspierać analizę logów z systemów operacyjnych posiadanych przez Zamawiającego, tj. Windows Serwer, Linux
		Rozwiązanie musi zapewniać raportowanie dla wszystkich przedmiotów dostępnych poprzez GUI systemu (np.: pobrane dane, zanalizowane dane, zdarzenia, przepływy, podatności, zasoby, zagrożenia, itp.). Rozwiązanie musi posiadać konfigurowalny silnik raportowania, tak aby możliwe było tworzenie

		niestandardowych raportów bez dodatkowych kosztów (licencje i wsparcie techniczne) usług ze strony producenta. Rozwiązanie musi zapewnić szablony do szybkiego tworzenia i dostarczania raportów na wielu poziomach szczegółowości.
		Rozwiązanie musi realizować analizę i sygnalizowanie incydentów nie tylko na zasadzie przekroczenia ustalonego progu dla zdarzeń, ale również na zasadzie analizy behawioralnej i oceny anomalii w trendzie. Rozwiązanie musi generować alerty na podstawie zauważonej zmiany w sieci dotyczącej pojawienia się nowej usługi lub gdy pojawią się nowe zasoby,
		Rozwiązanie musi posiadać zdolność korelowania zdarzeń z informacjami pozyskanymi ze znanych skanerów luk bezpieczeństwa
		Rozwiązanie musi wspierać różne standardy komunikacji, w celu przekazywania alertów do innych rozwiązań.
4	Monitorowanie i zarządzaniem sprzętem komputerowym oraz użytkownikami	Rozwiązanie musi umożliwiać wdrożenie pełnej wymaganej funkcjonalności na platformie wirtualizacyjnej. Dopuszcza się możliwość wykonania dostawy oprogramowania zbiorczego na urząd bądź dostarczone oprogramowanie musi obsługiwać przynajmniej 130 urządzeń (unikalnych adresów IP) w celu należytego monitorowania bezpieczeństwa urządzeń w sieci urzędu. Rozwiązanie w niniejszym zakresie musi udostępniać funkcjonalności: Audyt zasobów sprzętowych i oprogramowania: - Lista aplikacji oraz aktualizacji systemu operacyjnego na pojedynczej stacji roboczej (rejestr) - Lista aplikacji oraz aktualizacji systemu operacyjnego na pojedynczej stacji roboczej (skan dysków) - Numery seryjne (klucze) oprogramowania - Informacje o plikach wykonywalnych i wpisach rejestrowych na stacji roboczej - Informacje o plikach multimedialnych (mp3, avi itp.) oraz archiwach zip i ich metadanych (tytuł i autor utworu, zawartość pliku zip) - Ogólne informacje o sprzęcie stacji roboczej - Szczegółowe informacje o sprzęcie stacji roboczej (model, płyta, procesor, pamięć, napędy, karty itp.) - Informacje systemowe (komendy startowe, konta użytkowników, foldery udostępnione, informacje SMART itp.) - Audyt inwentaryzacji sprzętu i oprogramowania - Baza wzorców oprogramowania - Zarządzanie licencjami - Historia zmian sprzętu i oprogramowania - Środki Trwałe: baza ewidencji majątku IT (definiowanie własnych typów środków, ich atrybutów oraz wartości, załączniki, import danych z pliku CSV) - Alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych - Skaner inwentaryzacji offline - Skanowanie i drukowanie kodów kreskowych oraz QR
		Monitorowanie aktywności użytkowników: - Ogólne informacje o aktywności użytkownika - Szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy) - Użytkowane aplikacje (aktywnie i nieaktywnie, czyli całkowity czas działania aplikacji oraz czas faktycznego używania jej przez użytkownika) - Blokowanie uruchamianych aplikacji - Odwiedzane strony WWW (tytuły i adresy stron, ilość i czas wizyt) - Blokowanie stron WWW - Wydruki: audyt (per: drukarka, użytkownik, komputer), koszty wydruków - Wysłane i odebrane wiadomości e-mail (nagłówki) - Użycie łącza: generowany przez użytkowników ruch sieciowy (wchodzący i wychodzący, lokalny i internetowy) - Statyczny zdalny podgląd pulpitu użytkownika (bez dostępu) - Zrzuty ekranowe (historia pracy użytkownika "ekran po ekranie")
		Pomoc użytkownikom sieci: - Baza zgłoszeń serwisowych

		- Tworzenie zgłoszeń i zarządzanie zgłoszeniami (przypisywanie do administratorów z powiadamianiem e-mail) - Komentarze i załączniki w zgłoszeniach - Zrzuty ekranowe w zgłoszeniach - Wewnętrzny komunikator (czat) - Komunikaty wysyłane do użytkowników/komputerów z możliwym obowiązkowym potwierdzeniem odczytu - Statyczny zdalny podgląd pulpitu użytkownika (bez dostępu) - Zdalny dostęp do komputerów (pracownik, jak i administrator widzą ten sam ekran) z możliwym pytaniem użytkownika o zgodę - Zadania dystrybucji oraz uruchamiania plików (jeśli komputer jest wyłączony podczas uruchamiania dystrybucji, dojdzie ona do skutku po jego uruchomieniu) - Integracja bazy użytkowników z AD - Przypisywanie pracowników helpdesk do kategorii zgłoszeń - Procesowanie zgłoszeń z wiadomości e-mail - Baza wiedzy
		Kontrola dostępu użytkowników do urządzeń i nośników danych - Urządzenia podłączone do danego komputera - Lista wszystkich urządzeń podłączonych do komputerów w sieci - Audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych - Zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników (np. autoryzowanie firmowych szyfrowanych pendrive'ów, a blokowanie pendrive'ów prywatnych pracowników) - Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników AD - Integracja bazy użytkowników i grup z AD - Alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym
		Alarmowanie i raporty: - Alarmy zdarzenie-akcja (np. gdy ważne parametry znajdą się poza zakresem zdefiniowanym przez użytkownika) - Powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.) - Raporty (dla użytkownika, urządzenia, oddziału, mapy sieci lub całego atlasu)

Pakiet oprogramowania antywirusowego		
Lp.	**Parametr**	**Minimalne wymagania**
1	2	3
1	Przeznaczenie	Pakiet oprogramowania antywirusowego będzie stanowił element zwiększających bezpieczeństwo sieciowe w organizacji, tj. Wydziału Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami oraz serwerów na których będą uruchomione usługi przed złośliwym oprogramowaniem
2	Licencja	W ramach dostawy pakietu oprogramowania antywirusowego Zamawiający musi zostać wyposażony w: - zestaw oprogramowania wraz z licencjami umożliwiającymi scentralizowaną ochronę antywirusową sieci składającej się z 35 komputerów oraz serwerów, - dokumentację w postaci elektronicznej - w języku polskim, - Zamawiający wymaga, by dostarczone oprogramowanie było objęte 1 roczną opieką aktualizacyjną w zakresie udostępniania przez producenta nowych wersji oprogramowania oraz aktualizacji sygnatur. **UWAGA – parametr dodatkowo oceniany w kryterium wyboru oferty – Subskrypcja** Wydłużenie okresu opieki aktualizacyjnej w zakresie udostępniania przez producenta nowych wersji oprogramowania oraz aktualizacji sygnatur: • Subskrypcja: 12 miesięcy – 0 pkt,

		• Subskrypcja: 13 – 18 miesięcy – 2 pkt. • Subskrypcja: 19 – 24 miesięcy – 4 pkt. • Subskrypcja: 25 – 30 miesięcy – 6 pkt. • Subskrypcja: 31 – 35 miesięcy – 8 pkt. • Subskrypcja: 36 miesiące – 10 pkt.
3	Ogólne właściwości oprogramowania antywirusowego	- Oprogramowanie antywirusowe musi być dostępne w pakietach instalacyjnych dla stacji roboczych oraz serwerów. Dostarczane klucze licencyjne muszą pozwalać na aktywowanie oprogramowania przeznaczonego do ochrony stacji roboczych oraz serwerów. - Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami, ransomware i innymi potencjalnie niebezpiecznymi programami. - Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony. - Program ma mieć możliwość skanowania i klasyfikowania plików oraz odsyłaczy do zasobów sieciowych na podstawie informacji gromadzonych w oparciu o dane dostarczane przez producenta. - Program powinien chronić przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX). - Program ma mieć funkcję wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz innych narzędzi hakerskich. - Program ma mieć moduł skanujący pocztę przychodzącą i wychodzącą dla klienta poczty elektronicznej minimum Microsoft Office Outlook, który to program jest używany przez Zamawiającego. - Wbudowany moduł skanujący ruch HTTP w ma działać czasie rzeczywistym niezależnie od wykorzystywanej przez użytkowników przeglądarki WWW. - Program ma posiadać wbudowany moduł wyszukiwania heurystycznego - Program ma umożliwiać ochronę przed niebezpiecznymi rodzajami aktywności sieciowej oraz umożliwiać tworzenie reguł wykluczających dla określonych adresów/zakresów IP. - Program ma umożliwiać centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym za pośrednictwem modułu serwera oraz dostarczonego oprogramowania konsoli administratora. - Możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych. - Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. - Możliwość tworzenia list zaufanych procesów, dla których nie będzie monitorowana aktywność plikowa, aktywność aplikacji, nie będą dziedziczone ograniczenia nadrzędnego procesu, nie będzie monitorowana aktywność aplikacji potomnych, dostęp do rejestru oraz ruch sieciowy.
	Serwer oraz konsola zarządzania	Każdy z pakietów oprogramowania przeznaczonego zarówno na stacje robocze oraz serwery musi integrować się z konsolą zarządzania dostarczaną przez producenta oprogramowania antywirusowego. Pakiet instalacyjny systemu scentralizowanego zarządzania musi spełniać następujące wymagania: - System zdalnego zarządzania ma umożliwiać zarządzanie stacjami roboczymi i serwerami plików działającymi pod kontrolą systemów operacyjnych przynajmniej z rodziny Microsoft Windows/Linux posiadanych przez Zamawiającego. - Konsola administracyjna ma umożliwiać zdalne inicjowanie skanowania antywirusowego na kontrolowanych za jej pośrednictwem stacjach roboczych. - System centralnego zarządzania musi być wyposażony w mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych w sieci. - System zarządzania ma umożliwiać dystrybucję i instalowanie aktualizacji oprogramowania, który umożliwia automatyczne, przesłanie i zainstalowanie nowego oprogramowania na stacjach roboczych bez ingerencji ich użytkowników. - System musi posiadać moduł centralnego zbierania informacji i tworzenia sumarycznych raportów na temat zarejestrowanych zdarzeń. - System zdalnego zarządzania musi umożliwiać podgląd w czasie rzeczywistym statystyk ochrony, stanu aktualizacji komponentów oprogramowania antywirusowego, wykrytych zagrożeń itp.

		- System zdalnego zarządzania musi umożliwiać przeglądanie informacji o obiektach poddanych kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, skanowanie itp.). - System zdalnego zarządzania musi umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania. - System zdalnego zarządzania musi umożliwiać automatyczne instalowanie licencji oprogramowania antywirusowego na stacjach roboczych. - System zdalnego zarządzania powinien mieć możliwość sprawdzenia aktualnych wersji oprogramowania antywirusowego na serwerach i stacjach roboczych.

Zestaw certyfikatów kwalifikowalnych		
Lp.	**Parametr**	**Minimalne wymagania**
1	2	3
1	Certyfikaty kwalifikowalne	Zamawiający wymaga dostarczenia dla 5 osób Wydziału Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami kwalifikowanych podpisów elektronicznych na okres 2 lat wraz z kartą oraz czytnikiem lub kluczem USB