Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Umowa Nr ……..

zawarta w dniu …….. r. w …….. pomiędzy:
Gminą Młynary z siedzibą przy ul. Dworcowa 29, 14-420 Młynary,
NIP: 578-31-09-418**,** REGON: 170748130,
reprezentowaną przez**:**
Renatę Wiolettę Bednarczyk – Burmistrza Miasta i Gminy Młynary
Przy kontrasygnacie Katarzyny Rynkowskiej – Skarbnika Miasta i Gminy Młynary
zwaną/ym dalej „Zamawiającym”

…….. z siedzibą przy ul. …… w……,
NIP: **……**, REGON: **……..**
reprezentowana przez ……
zwaną/ym dalej „Wykonawcą”

zwane dalej wspólnie ”Stronami”.

§ 1
PRZEDMIOT UMOWY

1. Zakup sprzętu, oprogramowania i usług w celu zapewnienia warunków do zdalnej pracy oraz podniesienie poziomu cyberbezpieczeństwa w Urzędzie Miasta i Gminy w Młynarach w ramach konkursu „Cyfrowa Gmina" realizowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś Priorytetowa V: Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU.
2. Przedmiotem zamówienia, o którym mowa w ust.1 jest:
   a. Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS).
   b. Dostawa oprogramowania specjalistycznego OS x 2 szt.
   c. Dostawa oprogramowania specjalistycznego (program do tworzenia kopii) x 1 szt.
   d. Dostawa oprogramowania specjalistycznego (program do monitorowania sieci) x 1 szt.
   e. Dostawa stacji roboczych: typ 1 x 1 szt., typ 2 x 3 szt.
   f. Dostawa monitorów x 10 szt.
   g. Dostawa serwera komputerowego x 1 szt.
   h. Dostawa zasilaczy x UPS 10 szt.
   i. Dostawa oprogramowania roboczego x 10 szt.
   j. Dostawa urządzeń Acces point x 5 szt.
   k. Dostawa macierzy dyskowej x 1 szt.
   l. Przeprowadzenie szkolenia z cyberbezpieczeństwa dla pracowników Urzędu Miasta i Gminy w Młynarach do 30 osób.
   m. Dostawa infrastruktury teleinformatycznej (okablowanie, urządzenia aktywne, szafa z wyposażeniem).
3. Szczegółowy opis przedmiotu zamówienia wymienionego w pkt. 1.1. stanowi załącznik nr 1 do zapytania ofertowego.
4. Kompleksowa realizacja przedmiotu umowy musi być zgodna z wymaganiami określonymi w Szczegółowym Opisie będącym załącznikiem do niniejszej Umowy oraz Ofertą Wykonawcy.
5. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
6. W celu uniknięcia wątpliwości Strony potwierdzają, że z zastrzeżeniem zmian dopuszczalnych przez przepisy prawa i Umowę – przedmiot umowy zostanie zrealizowany zgodnie z treścią Szczegółowego Opisu oraz Ofertą Wykonawcy z uwzględnieniem wszelkich zmian oraz wyjaśnień

udzielonych w odpowiedzi na pytania Wykonawców, które miały miejsce w toku postępowania poprzedzającego zawarcie Umowy.

§ 2
SPOSÓB REALIZACJI PRZEDMIOTU UMOWY

1. Strony deklarują współpracę w celu realizacji Umowy. W szczególności Strony zobowiązane są do wzajemnego powiadamiania o ważnych okolicznościach mających lub mogących mieć wpływ na wykonanie Umowy, w tym na ewentualne opóźnienia.
2. Językiem Umowy i językiem stosowanym podczas jej realizacji jest język polski. Dotyczy to także całej komunikacji między Stronami.
3. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, by nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
4. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
5. Wykonawca zobowiązuje się wykonać przedmiot umowy z zachowaniem należytej staranności, przy wykorzystaniu całej posiadanej wiedzy i doświadczenia.
6. Wykonawca zgłosi gotowość do odbioru z wyprzedzeniem co najmniej 5 dni roboczych.
7. Odbiór przedmiotu umowy odbędzie się w Urzędzie Miasta i Gminy w Młynarach w obecności przedstawicieli obydwu Stron i polegać będzie na sprawdzeniu jego zgodności z wymaganiami SWZ, kompletności i stanu.
8. Wykonawca wyda Zamawiającemu dokumenty, które dotyczą sprzętu, przede wszystkim karty gwarancyjne i instrukcje obsługi sprzętu.
9. Odbiór przedmiotu umowy nastąpi na podstawie protokołu odbioru, który zostanie podpisany przez przedstawicieli Zamawiającego i Wykonawcy.
10. Protokół odbioru sporządzony zostanie w formie pisemnej, pod rygorem nieważności, w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron. O ile z Umowy lub przepisów prawa nie wynika inaczej, jedynie podpisany przez obie Strony Protokół odbioru jest podstawą do dokonania zapłaty odpowiedniej części wynagrodzenia. Zamawiający nie dopuszcza jednostronnych Protokołów odbioru wystawionych przez Wykonawcę.
11. Wykonawca oświadcza, że przedmiot umowy zostanie wykonany w zgodzie z prawem autorskim.
12. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.
13. Oferowane oprogramowanie musi pochodzić z oficjalnego kanału dystrybucji producenta.
14. Zamawiający zastrzega sobie możliwość weryfikacji legalności oprogramowania bezpośrednio u producenta w przypadku, jeśli poweźmie wątpliwości co do legalności jego pochodzenia.
15. Korzyści i ciężary związane ze sprzętem oraz niebezpieczeństwo przypadkowej utraty lub uszkodzenia sprzętu przechodzą na Zamawiającego z chwilą wydania sprzętu Zamawiającemu. Za dzień wydania sprzętu Zamawiającemu uważa się dzień, w którym sprzęt został odebrany przez Zamawiającego zgodnie z procedurą określoną w niniejszym paragrafie.
16. Potwierdzeniem terminowej realizacji przedmiotu umowy, o którym mowa w §1 ust. 1 jest protokół odbioru podpisany przez obie Strony.

§ 3
TERMIN WYKONANIA

1. Strony ustalają termin realizacji Umowy, tj. dostarczenie całości zaoferowanego sprzętu informatycznego wraz z oprogramowaniem oraz wymaganą instalacją i konfiguracją w ciągu **60 dni** od daty zawarcia Umowy, zgodnie z Ofertą Wykonawcy. Za datę zawarcia Umowy Zamawiający przyjmuje dzień, w którym zostanie ona podpisana przez obie Strony Umowy.
2. W uzasadnionych przypadkach termin określony w ust. 1 może ulec zmianie tylko za zgodą Zamawiającego. Zmiana terminu wymaga aneksu do Umowy.

3. Jeżeli w toku realizacji Umowy, mimo zachowania przez Wykonawcę należytej staranności, Wykonawca stwierdzi zaistnienie okoliczności dających podstawę do oceny, że przedmiot umowy nie zostanie wykonany w terminie określonym w ust. 1, niezwłocznie zawiadomi na piśmie Zamawiającego o przyczynach wystąpienia opóźnienia oraz przedstawi przewidywany termin dostawy.
4. Potwierdzeniem realizacji zamówienia w terminie, o którym mowa w ust. 1 jest protokół odbioru podpisany przez obie Strony.

§ 4
OBOWIĄZKI STRON

1. Zamawiający jest zobowiązany do współdziałania z Wykonawcą w granicach określonych prawem oraz Umową.
2. Wykonawca zobowiązany jest wykonać przedmiot umowy z najwyższą starannością, w sposób zgodny z:
    1) Szczegółowym Opisem;
    2) Ofertą Wykonawcy.
3. W celu uniknięcia wątpliwości przyjmuje się, że jeżeli Strony nie zdefiniowały danego działania niezbędnego do prawidłowej realizacji Umowy jako obowiązku Zamawiającego, Stroną zobowiązaną do wykonania takiego działania jest Wykonawca, jako podmiot profesjonalny. Powyższe ma zastosowanie w szczególności do elementów umożliwiających instalację i uruchomienie zakupionego sprzętu, np. kabli połączeniowych, zasilających, baterii itp.
4. Wykonawca zobowiązany jest wykonać przedmiot umowy z najwyższą starannością, wymaganą dla tego typu prowadzenia działalności gospodarczej.

§ 5
WYNAGRODZENIE

1. Łączne wynagrodzenie brutto za realizację przedmiotu umowy wynosi **…….. zł** (słownie: …… 00/100 złotych), w tym podatek VAT 23% - **…….. zł** (słownie: …… 00/100 złotych).
2. Strony ustalają, że podstawą do wystawienia przez Wykonawcę faktury jest należyte wykonanie obowiązków Wykonawcy wynikających z niniejszej Umowy, co musi zostać potwierdzone protokołami odbioru obejmującymi łącznie cały przedmiot umowy.
3. Za datę wykonania przedmiotu umowy w części lub w całości uważa się datę podpisania przez Zamawiającego odpowiedniego Protokołu odbioru (częściowego lub końcowego) bez zastrzeżeń, chyba że inna data została wskazana w Protokole odbioru. Protokół odbioru sporządzony zostanie w formie pisemnej, pod rygorem nieważności, w dwóch egzemplarzach, po jednym dla każdej ze Stron. O ile z Umowy lub przepisów prawa nie wynika inaczej, jedynie podpisany przez obie Strony Protokół odbioru jest podstawą do dokonania zapłaty odpowiedniej części wynagrodzenia. Zamawiający nie dopuszcza jednostronnych Protokołów odbioru wystawionych przez Wykonawcę.
4. Wynagrodzenie będzie płatne przelewem na rachunek bankowy Wykonawcy nr **……** w terminie do 30 dni od daty otrzymania prawidłowo wystawionej faktury VAT wraz z załączoną kopią Protokołów odbioru. Wynagrodzenie będzie płatne na rachunek Wykonawcy wskazany na fakturze.
5. Za datę zapłaty Strony ustalają dzień, w którym Zamawiający wydał bankowi polecenie przelewu wynagrodzenia na rachunek bankowy Wykonawcy.
6. Za opóźnienie w zapłacie faktur Zamawiający zapłaci odsetki ustawowe.
7. Zamawiający zastrzega sobie prawo rozliczania płatności wynikającej z Umowy z zastosowaniem mechanizmu podzielnej płatności, przewidzianego w przepisach ustawy o podatku od towarów i usług.
8. Wykonawca oświadcza, że rachunek bankowy wskazany w Umowie:
    1) jest rachunkiem umożliwiającym płatność z zastosowaniem mechanizmu podzielnej płatności, o którym mowa powyżej;

2) znajduje się w wykazie podmiotów prowadzonym przez Szefa Krajowej Administracji Skarbowej, o którym mowa w art. 96b ustawy o podatku od towarów i usług (tzw. biała lista podatników).

9. W przypadku, gdy rachunek bankowy Wykonawcy nie spełnia choćby jednego z warunków określonych w pkt. 8, opóźnienie w dokonaniu płatności w terminie określonym w umowie, powstałe wskutek braku możliwości:

1) realizacji przez Zamawiającego płatności wynagrodzenia z zastosowaniem mechanizmu podzielnej płatności i/lub

2) dokonania płatności na rachunek objęty wykazem podmiotów prowadzonym przez Szefa Krajowej Administracji Skarbowej, nie stanowi dla Wykonawcy podstawy do żądania od Zamawiającego jakichkolwiek odsetek/odszkodowań lub innych roszczeń z tytułu dokonania nieterminowej płatności.

§ 6
GWARANCJA

1. Wykonawca oświadcza, że udziela Zamawiającemu gwarancji jakości na dostarczone urządzenia na okres **i** na zasadach opisanych w Szczegółowym Opisie stanowiącym Załącznik nr 1 do zapytania ofertowego oraz zgodnie z Ofertą Wykonawcy.
2. Okres gwarancji biegnie od dnia podpisania protokołu odbioru przez Zamawiającego.
3. Gwarancja udzielona przez Wykonawcę nie wyłącza uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producentów sprzętu. Warunki gwarancji mają pierwszeństwo przed warunkami gwarancji udzielonych przez producentów sprzętu w zakresie, w jakim warunki gwarancji przyznają Zamawiającemu silniejszą ochronę.
4. Gwarancja udzielana jest w ramach wynagrodzenia.
5. W okresie gwarancji Wykonawca zapewnia serwis techniczny i nie może odmówić wymiany niesprawnej części na nową w przypadku, gdy jej naprawa nie gwarantuje prawidłowej pracy sprzętu, zgodnie z warunkami gwarancyjnymi.
6. Niezależnie od udzielonej gwarancji, Wykonawca ponosi wobec Zamawiającego odpowiedzialność za wady fizyczne i prawne przedmiotu umowy z tytułu rękojmi w terminie i na zasadach określonych w ustawie Kodeks cywilny.
7. Wykonawca ponosi wobec Zamawiającego odpowiedzialność za wady przedmiotu umowy z tytułu gwarancji jakości w terminie i na zasadach określonych w niniejszej Umowie, a w sprawach nieuregulowanych niniejszą umową przyjmuje się jako wiążące przepisy ustawy Kodeks cywilny.
8. Przez wadę należy rozumieć wadę fizyczną i prawną. Wada fizyczna rozumiana, jako jawne lub ukryte właściwości tkwiące w stanowiących przedmiot umowy dostawach lub w jakimkolwiek ich elemencie, powodujące niemożność używania lub korzystania z przedmiotu umowy zgodnie z przeznaczeniem, a także obniżenie jakości, uszkodzenia lub usterki w przedmiocie umowy. Wada prawna rozumiana, jako sytuacja w której przedmiot umowy lub jakikolwiek element przedmiotu umowy nie stanowi własności Wykonawcy albo jeżeli jest obciążony prawem osoby trzeciej, a także inne wady prawne.
9. Zgłoszenie awarii lub wady następuje telefonicznie/faxem na numer telefonu/faxu **…….. lub e-mailem na adres ……**
10. Jeśli dla danego elementu zamówienia nie postanowiono inaczej w SOPZ, Wykonawca potwierdzi zgłoszenie w ciągu 2 dni roboczych, a usunie awarię lub wadę w ciągu 14 dni kalendarzowych licząc od dnia zgłoszenia.

§ 7
KARY UMOWNE

1. W przypadku niewykonania lub nienależytego wykonania Umowy przez Wykonawcę Zamawiający może naliczyć karę umowną w następujących przypadkach i wysokościach:
1) za zwłokę w przekazaniu przedmiotu umowy w wysokości 100 zł za każdy dzień zwłoki;

2) za zwłokę w usunięciu awarii lub wad sprzętu w wysokości 0,1% ceny, o której mowa w § 5 ust. 1 Umowy za każdy dzień zwłoki w stosunku do terminów, o których mowa w § 6 ust. 10 Umowy;
3) za odstąpienie od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy w wysokości 10% wartości Umowy, o której mowa w § 5 ust. 1 Umowy.

2. Wykonawca może naliczyć karę umowną za odstąpienie od Umowy przez Wykonawcę z przyczyn leżących po stronie Zamawiającego w wysokości 10% wartości Umowy, o której mowa w § 5 ust. 1 Umowy z wyłączeniem przypadku, o jakim mowa w § 8 ust. 1 Umowy.
3. O nałożeniu kary umownej, jej wysokości i podstawie jej nałożenia Zamawiający będzie informował Wykonawcę pisemnie w terminie 14 dni od zaistnienia zdarzenia stanowiącego podstawę nałożenia kary.
4. Kary umowne liczone są od wynagrodzenia brutto należnego Wykonawcy.
5. Kwoty kar umownych będą płatne w terminie wskazanym w żądaniu Zamawiającego. Powyższe nie wyłącza możliwości potrącenia naliczonych kar, jak również zaspokojenia roszczeń z zabezpieczenia należytego wykonania Umowy lub potrącenia z wynagrodzenia należnego Wykonawcy.

§ 8
ODSTĄPIENIE OD UMOWY

1. Zamawiającemu przysługuje prawo odstąpienia od Umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy (zgodnie z art. 456 ustawy Prawo zamówień publicznych).
2. Zamawiający może odstąpić od Umowy ze skutkiem natychmiastowym również, gdy:
   1) Wykonawca pomimo pisemnego wezwania przez Zamawiającego i w terminie określonym w wezwaniu nie usunął stwierdzonych naruszeń oraz nie wykonuje zapisów Umowy zgodnie z jej postanowieniami lub w rażący sposób zaniedbuje bądź narusza zobowiązania umowne;
   2) nastąpiła niedopuszczalna zmiana składu Wykonawców, który wspólnie ubiegali się o udzielenie zamówienia i wspólnie je uzyskali;
   3) stwierdzenia w toku odbioru przedmiotu umowy, że przedmiot umowy zawiera wady i pomimo wyznaczenia terminu ich usunięcia Wykonawca ich nie poprawił lub nie przystąpił do ich usunięcia
   4) opóźnienie w realizacji przedmiotu umowy przekracza 14 dni.
3. Jeżeli Zamawiający nie współdziała z Wykonawcą w zakresie przewidzianym postanowieniami Umowy, a współdziałanie to jest konieczne do wykonania Umowy, Wykonawca jest uprawniony do odstąpienia od Umowy po uprzednim wezwaniu Zamawiającego do zapewnienia koniecznego współdziałania i wyznaczeniu mu w tym celu odpowiedniego terminu, nie krótszego niż 14 dni, z zagrożeniem odstąpienia od Umowy w razie jego bezskutecznego upływu. W wezwaniu Wykonawca zobowiązany jest wskazać dokładnie brak wymaganego współdziałania i jego wpływ na realizację Umowy. Wezwanie będzie wystosowane w formie pisemnej pod rygorem bezskuteczności wezwania.

§ 9
ZMIANY UMOWY

1. Zmiana Umowy dopuszczalna jest w zakresie i na warunkach przewidzianych przepisami ustawy Prawo zamówień publicznych, w szczególności:
   1) Strony są uprawnione do wprowadzenia do Umowy zmian nieistotnych, to jest innych, niż zmiany zdefiniowane w art. 454 ustawy Prawo zamówień publicznych;

2) stosownie do art. 455 ustawy Prawo zamówień publicznych, Zamawiający przewiduje możliwość wprowadzenia do Umowy następujących zmian w przypadku:

a. konieczności dostarczenia innego, niż określonego w Umowie urządzenia lub oprogramowania, niepowodująca zwiększenia ceny, spowodowana zakończeniem produkcji określonego w Umowie urządzenia/oprogramowania lub wycofania go z produkcji lub obrotu na terytorium Rzeczpospolitej Polskiej, posiadające parametry nie gorsze od zaproponowanych przez Wykonawcę w ofercie;

b. pojawienia się na rynku urządzenia producenta sprzętu nowszej generacji lub nowej wersji oprogramowania, o lepszych parametrach i pozwalających na zaoszczędzenie kosztów eksploatacji pod warunkiem, że te zmiany nie spowodują zwiększenia ceny;

c. ujawnienia się powszechnie występujących wad oferowanego urządzenia Zamawiający dopuszcza zmianę w zakresie przedmiotu umowy polegającą na zastąpieniu danego produktu produktem zastępczym, spełniającym wszelkie wymagania przewidziane w SOPZ dla produktu zastępowanego, rekomendowanym przez producenta lub Wykonawcę w związku z ujawnieniem wad;

d. zmiany przepisów prawa, opublikowanej w Dzienniku Urzędowym Unii Europejskiej, Dzienniku Ustaw, Monitorze Polskim lub Dzienniku Urzędowym odpowiedniego ministra, Zamawiający dopuszcza zmiany sposobu realizacji Umowy lub zmiany zakresu świadczeń Wykonawcy wymuszone takimi zmianami prawa;

e. zmiany Podwykonawcy, przy pomocy którego Wykonawca realizuje przedmiot umowy, po uprzedniej akceptacji Zamawiającego;

f. wystąpienia siły wyższej.

2. W przypadkach, w których zgodnie z powyższymi postanowieniami lub przepisami prawa możliwe jest wprowadzenie zmiany do Umowy, Zamawiający przewiduje także wprowadzenie odpowiedniej zmiany terminu realizacji, w szczególności:

1) o ile zmiana taka jest konieczna w celu prawidłowego wykonania Umowy, w szczególności ze względu na zaistnienie okoliczności, o których mowa w ust. 1 pkt 2;

2) ze względu na okoliczności niezależne od Wykonawcy, np. opóźnienie w dostawie z zagranicy, kontrola celna, opóźnienie lub zatrzymanie transportu wynikające, np. z powodów warunków atmosferycznych.

3. Strony postanawiają, że w przypadku zmiany stawki podatku od towarów i usług – wynagrodzenie przewidziane niniejszą Umową ulegnie zmianie odpowiedniej do zmiany wysokości podatku od towarów i usług (ulegnie korekcie o wysokość zmiany podatku VAT), przy czym powyższa zmiana będzie miała zastosowanie wyłącznie w odniesieniu do części wynagrodzenia objętego fakturami wystawionymi po dacie wejścia w życie zmiany przepisów prawa wprowadzających nowe stawki podatku od towarów i usług.

4. Nie stanowi zmiany Umowy zmiana danych rejestrowych lub adresowych oraz ich danych kontaktowych.

§ 10
POSTANOWIENIA KOŃCOWE

1. Wykonawca nie ma prawa dokonywać cesji, przeniesienia bądź obciążenia swoich praw lub obowiązków wynikających z Umowy bez uprzedniej pisemnej zgody Zamawiającego, udzielonej na piśmie pod rygorem nieważności.

2. Umowa zawarta jest pod prawem polskim. Wszelkie spory będą poddane pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby Zamawiającego.

3. W sprawach nieuregulowanych niniejszą Umową stosuje się przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U. 2020 poz. 1740 z późn. zm.).

4. Wszelkie zmiany Umowy będą dokonywane za zgodą obu Stron, w formie pisemnej pod rygorem nieważności. Zmiany będą dokonywane w postaci aneksów do Umowy, chyba że w Umowie wskazano inaczej.

5. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, jeden dla Wykonawcy, a dwa dla Zamawiającego.
6. Integralną część Umowy stanowią następujące Załączniki:
   1) Szczegółowy opis przedmiotu zamówienia.
   2) Oferta Wykonawcy.

Zamawiający

Wykonawca

Załącznik nr 1 do umowy nr ……
z dnia ……..

Szczegółowy opis			**Parametry oferowane**
Rozbudowę zabezpieczeń logicznych (firewall, systemy IDS, IPS) – 1 szt. W ofercie należy podać nazwę producenta, typ oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. Jeśli na stronie internetowej producenta nie jest dostępna pełna oferta modeli sprzętu wraz z jego konfiguracją, do oferty należy dołączyć katalog producenta zaoferowanego produktu umożliwiający weryfikację oferty pod kątem zgodności z wymaganiami Zamawiającego. Nie dopuszcza się zaoferowania komputera refurbished.			Producent: Model:
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.			
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.			Linki stron producenta umożliwiające weryfikacje
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
1.	**Redundancja, monitoring i wykrywanie awarii**	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN.	
2.	**Interfejsy, Dysk, Zasilanie:**	1. System realizujący funkcję Firewall musi dysponować minimum: • 5 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie	

		modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.	
3.	**Parametry wydajnościowe:**	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps. 5. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps. 6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps. 7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.	
4.	**Funkcje Systemu Bezpieczeństwa:**	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą	

		zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system	
5.	**Polityki, Firewall**	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.	
6.	**Połączenia VPN**	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.	

		• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.	
7.	**Routing i obsługa łączy WAN**	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	
8.	**Funkcje SD-WAN**	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.	
9.	**Zarządzanie pasmem**	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	
10.	**Ochrona przed malware**	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi	

		serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	
11.	**Ochrona przed atakami**	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
12.	**Kontrola aplikacji**	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	
13.	**Kontrola WWW**	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.	

		3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.	
14.	**Uwierzytelnianie użytkowników w ramach sesji**	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	
15.	**Zarządzanie**	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.	

		6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	
16.	**Logowanie**	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.	
17.	**Certyfikaty**	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.	
	Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.	
	Gwarancja oraz wsparcie	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	

Zakup specjalistycznego oprogramowania -OS MS Windows Server 2022 Standard z licencją na odpowiednią liczbę oferowanych rdzeni w serwerze i 4 wirtualnych maszyn lub równoważny tj. : • współpraca z procesorami o architekturze x86-64 • instalacja i użytkowanie aplikacji 32-bit. i 64-bit. • praca w roli serwera domeny Microsoft Active Directory • zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP) • zawarta możliwość uruchomienia roli serwera DNS • zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP) • zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory - zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory - zawarta możliwość uruchomienia roli serwera stron WWW • w ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera - w ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych • wszystkie wymienione parametry, role, funkcje, itp. Systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów)	
• Oryginalny Nośnik z zawartością systemu instalacyjnego oraz kluczem produktu • Nie dopuszcza się zaoferowania licencji refurbished.	

Zakup specjalistycznego oprogramowania Oprogramowanie posiada budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., są odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Są one również grupowane w osobnym, dedykowanym oknie. Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów są logowane oznacza to, że program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie: a) wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping b) wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU) c) wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci d) wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła. e) wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku. f) wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze. g) wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie. h) wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny. i) zablokowania mapy urządzeń przed przypadkową edycją. j) serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. k) serwerów pocztowych: l) monitorowania serwerów WWW i adresów URL.	

m) cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS. n) obsługi szyfrowania SSL/TLS w powiadomieniach e-mail. o) obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID. p) obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych. q) monitoringu routerów i przełączników r) serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie. s) wydajności systemów Windows: Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). W ZAKRESIE INWENTARYZACJI program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz: 1. Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. 2. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 3. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. 4. Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 5. Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. 6. Umożliwia odczytanie numeru seryjnego (klucze licencyjne). 7. Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 8. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.	

9. Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 10. Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane. Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania: • przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz • automatycznego aktualizowania zgromadzonych informacji, • tworzenia powiązań między zasobami a urządzeniami, • tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak • i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych, • wskazania osób uprawnionych do użycia zasobów, • definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz, • określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, • określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, • definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, • importu danych z zewnętrznego źródła (.CSV), • przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury • zakupu, gwarancji, dowolnego dokumentu itp., • tworzenia powiązań między zasobami a dokumentami w relacji 1:N, • oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., • ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, • konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie • czynności, • generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich • oprogramowania, • przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania • zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, • konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego	

• wzorca, • konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg • zdefiniowanego wzorca, • archiwizacji i porównywania audytów zasobów, • tworzenia kodów kreskowych dla zasobów, • drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla • zasobów, które posiadają numer inwentarzowy, • inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, • inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez • manualne wykonanie skanów inwentaryzacji offline), • definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” • z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”). 11. Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. 12. Zarządzanie posiadanymi licencjami: raport zgodności licencji. 13. Możliwość przypisania do programów numerów seryjnych, wartości itp. W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program umożliwia monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie: • Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), • Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach, • Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, • Informacji o edytowanych przez użytkownika dokumentach, • Historii pracy (cykliczne zrzuty ekranowe), • Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt), • Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), • Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość	

„grupowania” drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
- Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program ponadto posiada możliwość:

- blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
- blokowania ruchu na wskazanych portach TCP/IP,
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,
- przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.

PROGRAM UMOŻLIWIA REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM.

W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia

takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu

zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością jest umożliwienie

użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z

administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł ten zawiera również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym. Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika. Moduł pomocy zdalnej umożliwia również: • pobieranie listy użytkowników z Active Directory, • zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, • zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń, zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej, • tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, • automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,	

• procesowanie zgłoszeń użytkowników z wiadomości e-mail, • tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, wykonywanie operacji na wielu zgłoszeniach równocześnie, dołączanie załączników do zgłoszeń, rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, • szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, • wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, • zrzuty ekranowe (podgląd pulpitu), • dystrybucję oprogramowania przez Agenty, • dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), • zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, • możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, • planowanie nieobecności pracowników helpdesk, • obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, • generowanie raportów obsługi helpdesk, • zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), • zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), • wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików. MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM poprzez blokowanie urządzeń. 1. Blokowanie urządzeń i nośników danych. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane. 5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.	

7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 8. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. 9. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM. Zarządzanie prawami dostępu do urządzeń: 1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. urządzenia prywatne są blokowane. 3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane. Audyt operacji na plikach na urządzeniach przenośnych: 1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 2. Podłączenie/odłączenie urządzenia przenośnego. 3. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. 4. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. 5. Przydzielanie uprawnień również do kont użytkowników lokalnych Licencja ma obejmować 35 komputerów ze wsparciem i aktualizacjami na 12 m-cy	

Stacja Robocza typ 1 – 1 szt. Komputer będzie wykorzystywany dla potrzeb aplikacji graficznych, bazy danych oraz monitorujących dlatego zaoferowany sprzęt musi być przystosowany do pracy ciągłej. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji w oparciu o materiały i systemy dostępne na stronie producenta – załączyć link do strony/systemu Typ gdzie można dokonać weryfikacji.	Producent: Model:
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
1.	Obudowa	Typu Tower z obsługą kart PCI Express o niskim profilu: - 1 x PCI Express 4.0 x16, - 2 x PCI Express 3.0 x1, Wyposażona w min: - 1 szt. 5,25" (dopuszcza się zastosowanie jednej kieszeni 5,25" w wersji SLIM dla napędu optycznego) - 1 szt. 3,5" + 1 szt. 2,5'' lub 2 szt. 2,5" Obudowa musi być wyposażona w czujnik otwarcia. Wbudowany głośnik o mocy 2W Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem konfiguracji, numerem seryjnym	
2.	Chipset	Dostosowany do zaoferowanego procesora	
3.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w min. 2 złącza M.2 z czego 1 dedykowane dla dysku SSD PCIe.	
4.	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych lub stacjach roboczych klasy x86, o wydajności liczonej w punktach równej lub wyższej niż 19 950 pkt. na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/. Wykonawcac w składanej ofercie winien podać dokładny model oferowanego podzespołu.	
5.	Pamięć operacyjna	16GB, 3200MHz DDR4, 4 sloty na pamięć, z czego min. 3 wolne. Praca pamięci w trybie dual channel. Możliwość rozbudowy pamięci do 128GB RAM.	
6.	Konfiguracja dyskowa	Min 512GB M.2 PCIe, wspierający sprzętowe szyfrowanie dysku, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość zainstalowania do 3 dysków	
7.	Karta graficzna	Karta graficzna dedykowana posiadające min. 8GB pamięci RAM DDR5, osiągająca wydajności liczonej w punktach min. 13 500 pkt. na podstawie testu Passmark G3D według wyników opublikowanych na stronie www.videocardbenchmark.net/ Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.	
8.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.	
9.	Karta sieciowa	Karta sieciowa LAN obsługująca prędkości 10/100/1000 wspierająca WoL	
10.	Porty/złącza	Wbudowane porty: - 1 x HDMI, - 2 x DP, - 8 x USB-A w tym min.: 4x USB 3.2 z przodu obudowy - port sieciowy RJ-45, - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	

11.	Klawiatura/mysz	Klawiatura przewodowa w układzie US lub EU, Mysz przewodowa (scroll),	
12.	Zasilacz	Energooszczędny zasilacz o mocy min. 380W oraz sprawności na poziomie min. 92%.	
13.	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.	

		16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb „kiosk”. 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).” 24. Wbudowany mechanizm wirtualizacji typu hypervisor.” 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM	

		33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń	
14.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.	
15.	BIOS	Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera - numerze konfiguracji, - numerze seryjnym, - numerze inwentarzowym (tzw. Asset Tag), - MAC Adres karty sieciowej, - zainstalowanej licencji w BIOS na system operacyjny OEM, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora na procesorze - stanie pracy wentylatora w obudowie komputera - napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego) Możliwość z poziomu Bios: - wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy - wyłączenia selektywnego (pojedynczego) portów SATA,	

		- wyłączenia karty sieciowej, karty audio, portu szeregowego, - możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora - wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze) z możliwością czyszczenia logów - alertowania zmiany konfiguracji sprzętowej komputera - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - załadowania optymalnych ustawień Bios bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.	
16.	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego • test monitora • test magistrali PCI-e • test portów USB • test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku uszkodzenia bądź błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja oraz data wydania Bios • Procesor: Nazwa, taktowanie • Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy • Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.	
17.	Certyfikaty i standardy	- Certyfikat ISO9001 dla producenta sprzętu - Energy Star min. 8.0 - Certyfikat TCO - Deklaracja zgodności CE - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji	

		substancji niebezpiecznych w postaci oświadczenia producenta jednostki	
18.	Bezpieczeństwo	- Złącze typu Kensington Lock Moduł TPM 2.0 z certyfikacją TCG	
19.	Gwarancja	2 lata świadczona w miejscu użytkowania sprzętu (on-site) Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń - Zamawiający zastrzega sobie prawo do możliwości weryfikacji powyższego wymogu. W przypadku weryfikacji przez Zamawiającego, Wykonawca dostarczy stosowne dokumenty pochodzące od producenta komputera. Wymagane oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.	
20.	Wsparcie techniczne producenta	- możliwość weryfikacji u producenta konfiguracji fabrycznej i oferowanej zakupionego sprzętu - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
21.	Wymagania dodatkowe	Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 14 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu.	

Stacja Robocza typ 2 – 3 szt. Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.			Producent: Model:
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.			
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
22.	Obudowa	Typu Small Form Factor (SFF) z obsługą kart PCI Express wyłącznie o niskim profilu. Wyposażona w min.: 1 szt. 5,25” zewnętrzną zatokę (dopuszcza się w wersji tzw slim zajętej przez napęd optyczny), 2 szt. 3,5” lub 2,5”, możliwość rozbudowy komputera do konfiguracji min. trzydyskowej w oparciu o dyski w rozmiarach 2,5” lub 3,5” + M.2. Obudowa musi być wyposażona w czujnik otwarcia obudowy	

		Sloty min.: - 1 x PCI Express x16, - 1 x PCI Express x1, Wbudowany głośnik o mocy 1W Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem konfiguracji, numerem seryjnym	
23.	Chipset	Dostosowany do zaoferowanego procesora	
24.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w min. 2 złącza M.2 z czego 1 dedykowane dla dysku SSD PCIe.	
25.	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności liczonej w punktach równej lub wyższej niż 10 950 pkt. na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.	
26.	Pamięć operacyjna	8 GB, 3200MHz DDR4, 4 sloty na pamięć, z czego min. 3 wolne. Możliwość pracy pamięci w trybie dual channel. Możliwość rozbudowy pamięci do 128GB RAM.	
27.	Konfiguracja dyskowa	Min 256GB M.2 PCIe, wspierający sprzętowe szyfrowanie dysku, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
28.	Napęd optyczny	Nagrywarka DVD +/-RW	
29.	Karta graficzna	Zintegrowana karta graficzna z procesorem.	
30.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.	
31.	Karta sieciowa	Karta sieciowa LAN obsługująca prędkości 10/100/1000	
32.	Porty/złącza	Wbudowane porty: - 1 x HDMI, - 2 x DP, - 8 x USB-A w tym min.: 4x USB 3.2 z przodu obudowy - 1 x USB-C z przodu obudowy - port sieciowy RJ-45, - port szeregowy RS-232 - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy - czytnik kart pamięci Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	

33.	Klawiatura/mysz	Klawiatura w układzie US + mysz optyczna z rolką	
34.	Zasilacz	Energooszczędny zasilacz o mocy nie większej niż 180W oraz sprawności na poziomie min. 85%.	
35.	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.	

		14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb „kiosk“. 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).“ 24. Wbudowany mechanizm wirtualizacji typu hypervisor.“ 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu	

		plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń	
36.	BIOS	Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera	

		- numerze konfiguracji, - numerze seryjnym, - numerze inwentarzowym (tzw. Asset Tag), - MAC Adres karty sieciowej, - zainstalowanej licencji w BIOS na system operacyjny OEM, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora na procesorze - stanie pracy wentylatora w obudowie komputera - napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego) Możliwość z poziomu Bios: - zmiany ustawienia kontrolera z trybu AHCI na RAID i odwrotnie, - wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia karty sieciowej, karty audio, portu szeregowego, - możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora - wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów - alertowania zmiany konfiguracji sprzętowej komputera - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania trzech sekwencji bootujących (podstawowa, WOL, po awarii) - załadowania optymalnych ustawień Bios bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń	

		zewnętrznych.	
37.	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego • test monitora • test magistrali PCI-e • test portów USB • test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku uszkodzenia bądź błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja oraz data wydania Bios • Procesor: Nazwa, taktowanie • Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy • Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.	
38.	Certyfikaty i standardy	- Certyfikat ISO9001 dla producenta sprzętu (należy załączyć do oferty) - Certyfikat ISO14001 dla producenta sprzętu (należy załączyć do oferty) - Certyfikat ISO50001 dla producenta sprzętu (należy załączyć do oferty) - Epeat Silver - Energy Star min. 8.0 - Certyfikat TCO - Deklaracja zgodności CE (załączyć do oferty) - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki	
39.	Bezpieczeństwo	Złącze typu Kensington Lock Moduł TPM 2.0	

40.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.	
41.	Gwarancja	24 miesięcy door to door Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń - Zamawiający zastrzega sobie prawo do możliwości weryfikacji powyższego wymogu. W przypadku weryfikacji przez Zamawiającego, Wykonawca dostarczy stosowne dokumenty pochodzące od producenta komputera. Wymagane oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.	
42.	Wsparcie techniczne producenta	- możliwość weryfikacji u producenta konfiguracji fabrycznej i oferowanej zakupionego sprzętu - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
43.	Wymagania dodatkowe	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca.	

Monitor - 10 szt			Producent: Model:
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.			
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
44.	Przekątna	Min. 23,8”	

45.	Rozdzielczość	Min. 1920x1080	
46.	Ekran	Min. VA lub IPS z funkcją Low Blue Light i Flicker-Free	
47.	Jasność	Min. 250 cd/m	
48.	Czas reakcji	Maks. 4ms	
49.	Kąty widzenia	Min. 178/178 poziomo/pionowo	
50.	Regulacja kąt pochylenia	min. 20 stopnie w górę oraz min. 5 stopni w dół	
51.	VESA	Min. 100x100 mm	
52.	Porty Wbudowane	HDMI, DVI, AUDIO-IN	
53.	Głośniki	Wbudowane 2 x 1,5W	
54.	Pobór mocy w trybie pracy	max. 20W, W trybie czuwania max. 0,5 W	
55.	Certyfikaty	CE, ROHS	
56.	Gwarancja	24 miesięcy	

Serwer komputerowy - 1 szt.			Producent: Model:
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.			
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
57.	Obudowa	Obudowa: typu rack o wysokości 1U pozwalająca na montaż min. 4 dysków 3.5” Hot-Plug oraz dodatkowo umożliwiająca instalację klatki umieszczonej w tylnej części serwera na co najmniej dwa dyski 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI	
58.	Procesor	Zainstalowany jeden procesor min 12-rdzeniowe, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku 23 200 w teście CPU Average CPU Mark dostępnym na stronie https://www.cpubenchmark.net/ (Załączyć do oferty wydruk ze strony potwierdzający osiągany wynik - stan nie wcześniej niż dzień ogłoszenia postępowania). Procesory musza posiadać obsługę technologii wirtualizacji.	

59.	Płyta główna:	Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna zaprojektowana przez producenta i oznaczona jego znakiem firmowym.	
60.	Chipset:	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	
61.	Pamięć operacyjna:	min. 32GB DDR4 3200MT/s, na płycie znajduje się min. 16 sloty przeznaczone do instalacji pamięci. Płyta obsługuje do 1TB Pamięci RAM.	
62.	Wsparcie dla następujących technologii zabezpieczeni a pamięci:	Memory Rank Sparing, Memory Mirror, Lockstep.	
63.	Gniazda PCI:	Min. 2 sloty PCIe x16 generacji 4	
64.	Interfejsy sieciowe:	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w wymaganych slotach PCIe). Dodatkowa karta sieciowa wyposażona w min. 2 interfejsy 10Gb Ethernet w standardzie SFP+. Ponadto 2 wkładki SFP+ wielomodowe (+ niezbędne okablowanie do połączenia) kompatybilne z serwerem i przełącznikami oferowanymi w zamówieniu.	
65.	Kontroler RAID:	Zainstalowany sprzętowy kontroler dysków SAS/SATA z funkcjonalnością RAID 0,1,10. Możliwość zainstalowania karty obsługującej co najmniej dwa dyski M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Wsparcie dla dysków samoszyfrujących.	
66.	Dyski twarde:	możliwość instalacji dysków SAS, SATA, SSD; Zainstalowane dyski: 2 dyski twarde o pojemności min. 480GB SSD (Hot-Plug)	
67.	Video:	Zintegrowana karta graficzna umożliwiająca wyświetlanie rozdzielczości min. 1280x1024;	
68.	Zasilanie:	Zainstalowane dwa zasilacze max. 800W (każdy) Hot-Plug. Dostarczone kable zasilające min. 2 m.	
69.	Wbudowane porty:	min. 3xUSB, w tym min. 1 port USB 3.0; min. 2 porty VGA z czego 1 na panelu przednim; min. jeden port typu serial; min. 1 port RJ45 pod zarządzanie.	
70.	Karty sieciowe:	Wbudowane dwa porty 1Gb Ethernet, dodatkowy moduł 2x10Gb SFP+ nie zajmujący slotów PCie wraz z 2 wkładkami 10GbE SFP+ do komunikacji z przełącznikami (wymagane 2 kpl).	

71.	Bezpieczeństwo:	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą; Moduł TPM 2.0.	
72.	Zdalne zarządzanie:	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; - wsparcie dla IPv6; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - integracja z Active Directory; - wsparcie dla dynamic DNS; - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera Oprogramowanie do zarządzania: - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; - integracja z Active Directory; - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; - Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish; - Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; - Szczegółowy opis wykrytych systemów oraz ich komponentów; - Możliwość eksportu raportu do CSV, HTML, XLS, PDF; - Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu; - Grupowanie urządzeń w oparciu o kryteria użytkownika; - Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji; - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach; - Szybki podgląd stanu środowiska; - Podsumowanie stanu dla każdego urządzenia; -Szczegółowy status urządzenia/elementu/ komponentu; -Generowanie alertów przy zmianie stanu urządzenia; -Filtry raportów umożliwiające podgląd najważniejszych zdarzeń; - Integracja z service desk producenta dostarczonej platformy sprzętowej; - Możliwość przejęcia zdalnego pulpitu; - Możliwość podmontowania wirtualnego napędu; - Kreator umożliwiający dostosowanie akcji dla wybranych alertów; - Możliwość importu plików MIB;	

		- Przesyłanie alertów „as-is” do innych konsol firm trzecich; - Możliwość definiowania ról administratorów; - Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów; - Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); - Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta; - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; - Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.; - Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności; - Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile; - Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami; - Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta; - Zdalne uruchamianie diagnostyki serwera; - Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym; - Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V;	
73.	Gwarancja:	minimum 24 miesiące lub dłużej zgodnie ze złożoną ofertą gwarancji producenta z czasem reakcji w następnym dniu roboczym, gwarancja realizowana w miejscu użytkowania sprzętu. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.	
74.	Certyfikaty i dokumenty:	Zamawiający wymaga dołączenia do oferty poniższych dokumentów: • Certyfikat ISO 50001 lub równoważny dla producenta serwera; • Certyfikat ISO 14001 lub równoważny dla producenta serwera; • Certyfikat ISO 9001 lub równoważny producenta o produkowaniu sprzętu zgodnie z tą normą;	

		• Certyfikat ISO 9001 na świadczenie usług serwisowych oraz posiadanie autoryzacji producenta urządzeń dla firmy serwisującej; • Serwer musi posiadać deklaracja CE. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów x64, Microsoft Windows Server 2022, Microsoft Windows Server 2019. • Oświadczenia Producenta, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta oraz, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.	

Zasilacz - 10 szt			Producent: Model:
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.			
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
75.	Moc pozorna	650 VA	
76.	Architektura UPS-a	line-interactive	
77.	Liczba faz na wejściu	1 (230V)	
78.	Czas przełączenia (maks.)	4 ms	
79.	Czas ładowania	6 h	
80.	Typ obudowy	Tower	
81.	Zabezpieczenia / filtry:	Przeciwprzepięciowe, Przeciwzakłóceniowe, Linii danych	
82.	Porty zasilania we.	Typ F Schuko	
83.	Porty zasilania wy.	3 x typ C/E	
84.	Gwarancja	24 miesięcy	

Oprogramowanie robocze - 10 szt.	Producent:

	Model:
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.	
Microsoft Office Home & Business 2019 lub równoważny Pakiet biurowy Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej. 2. Wymagania odnośnie interfejsu użytkownika: a. Pełna polska wersja językowa interfejsu użytkownika. b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. 3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: a. Posiada kompletny i publicznie dostępny opis formatu. b. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 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. c. Pozwala zapisywać dokumenty w formacie XML. 4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb Zamawiającego. 5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). 6. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim. 7. Pakiet zintegrowanych aplikacji biurowych musi zawierać: a. Edytor tekstów. b. Arkusz kalkulacyjny. c. Narzędzie do przygotowywania i prowadzenia prezentacji. d. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami). 8. 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. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. j. Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu. k. Wydruk dokumentów. l. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. m. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010, 2013, 2016 i 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu. . Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. o. Wymagana jest dostępność do oferowanego edytora tekstu	

bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem. p. Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. 9.rkusz 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). e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narędzia 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. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010, 2013, 2016 i 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. 10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a. Przygotowywanie prezentacji multimedialnych, które będą: b. Prezentowanie przy użyciu projektora multimedialnego. c. Drukowanie w formacie umożliwiającym robienie notatek. d. Zapisanie jako prezentacja tylko do odczytu. e. Nagrywanie narracji i dołączanie jej do prezentacji. f. Opatrywanie slajdów notatkami dla prezentera. g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo. h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. j. Możliwość tworzenia animacji obiektów i całych slajdów. k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010, 2013, 2016 i 2019. 11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych. c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. e. Automatyczne grupowanie wiadomości poczty o tym samym tytule. f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.	

. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów. h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie. i. Zarządzanie kalendarzem. j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników. k. Przeglądanie kalendarza innych użytkowników. l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. m. Zarządzanie listą zadań. n. Zlecanie zadań innym użytkownikom. o. Zarządzanie listą kontaktów. p. Udostępnianie listy kontaktów innym użytkownikom. q. Przeglądanie listy kontaktów innych użytkowników. r. Możliwość przesyłania kontaktów innym użytkowników. s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http. Infrastruktura teleinformatyczna (okablowanie, urządzenia aktywne, szafa z wyposażeniem 13000	

Acces point - 5 szt			Producent: Model:
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.			
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
85.	Porty we/wy	1 x 10/100/1000 Mbit/s PoE	
86.	Pasmo	2,4 GHz 5 GHz	
87.	Architektura sieci	GigabitEthernet	
88.	Standardy	802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax, 802.3af, 802.1Q	
89.	Liczba anten	min 1	
90.	Antena	ewnętrzna	
91.	Zysk anteny	Min 3 dBi	
92.	Certyfikaty	CE, FCC, IC	
93.	Zarządzanie, monitorowanie, konfiguracja:	BSSID 8 na radio, VLAN 802.1Q, Zaawansowane QoS Ograniczenie stawki zaużytkownika, Izolacja Guest Trafc Utrzymany	
94.	Bezpieczeństwo	WPA / WPA2 / WPA3	
95.	Metoda zasilania:	802.3af PoE, pasywne PoE (48 V)	
96.	Zestaw montażowy:	sufit/ściana	
97.	Obsługiwane szybkości transmi	802.11a 6, 9, 12, 18, 24, 36, 48, 54 Mb / s 802.11n (Wi-Fi 4) 6,5 Mb / s do 300 Mb / s (MCS0 - MCS15, HT 20/40) 802.11b 1, 2, 5,5, 11 Mb / s 802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mb / s	

	sji danych (Mbps)	802.11ac (Wi-Fi 5) 6,5 Mb / s do 866,7 Mb / s (MCS0 - MCS9 NSS1 / 2, VHT 20/40/80) 802.11ax (Wi-Fi 6) 6,3 Mb / s do 1,2 Gb / s (MCS0 - MCS11 NSS1 / 2, HE 20/40/80)	
98.	Gwarancja	24 miesiące	

Macierz dyskowa - 1szt			Producent: Model:
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.			
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
99.	Pamięć systemowa	min. 8GB DDR4	
100	Obudowa:	max. 1U wraz z szynami umożliwiającymi montaż serwera w szafie rack,	
101	Procesor	4 rdzeniowy	
102	pamięć flash	min. 4 GB,	
103	wnęka dysków	min. 4 x 3,5” SATA 6 Gb/s	
104	port LAN	min. 2x 10 GbE SFP+,	
105	port LAN	min. 2x min. 1 GbE RJ45,	
106	port USB	min. 4 x USB w tym min. 2 x USB gen.3.1,	
107	zasilacz	max. 100 W,	
108	Funkcje	hot swap RAID 0/1/5/6/10. Przywracanie RAID. Migracja Poziomów RAID.	
109	Kopia	na dyski zewnętrzne i inne urządzenia.	
110	Zainstalowane:	min. 2 dyski o pojemności min. 240GB SSD NVMe M.2, 4 dyski o pojemności min. 6TB SATA 6 Gb/s 7200 RPM, bufor 256 MB, czas pracy MTBF 2 000 000.	
111	Inne wymagania:	Buforowanie SSD, Nadmiarowa alokacja SSD Migawka/kopia zapasowa jednostek iSCSI LUN, Kontroler domeny i serwer NTP, Wolumin z elastycznym alokowaniem, Jednostki iSCSI LUN oparte na blokach, Odzyskiwanie miejsca, Funkcja typu Storage Plug & Connect (iSCSI i CIFS), Obsługa ACL na poziomie folderów współdzielonych, Kopie Migawkowe, Replikacja zdalna w czasie rzeczywistym, Replikacja zdalna (rsync), Oprogramowanie do tworzenia kopii zapasowych, Obsługa etykiet woluminu na dyskach zewnętrznych, Uwierzytelnianie AD,	

		Serwer i klient LDAP, Powiadomienia (e-mail), Kosz sieciowy, SNMP, Logowanie administratora przez Telnet i SSH, Gwarancja 24 miesięcy.	

Szkolenie z cyberbezpieczeństwa – dla personelu UMIG do 30 osób	
Dopuszcza się przeprowadzenie szkolenia w formie online. Szkolenie dla grupy 30 osób, zakończone wydaniem stosownych zaświadczeń potwierdzających uczestnictwo w szkoleniu.	

Infrastruktura teleinformatyczna	Producent: Model:
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.	
1. Szczegółowy opis montażu elementów wyposażenia serwerowni. 2. Montaż i konfiguracja sprzętu muszą być wykonane w godzinach i dniach wolnych od pracy Zamawiającego, w godzinach 16:00 do 6:00 lub w weekendy. W terminach uzgodnionych z Zamawiającym. 3. Doposażenie pomieszczenia serwerowni w szafę serwerową wraz z niezbędnym wyposażeniem do organizacji infrastruktury teleinformatycznej (patchpanele, zaślepki, organizatory, półki) Min .wymagania: - wysokość robocza: 42U, - szerokość montażowa: 19'', - wymiary [mm] (szerokość x głębokość x wysokość): 800x1000x2055, - kolor: czarny - drzwi przednie: pojedyncze metalowe - stal perforowana, drzwi tylne: pojedyncze metalowe - pełna stal, jakość certyfikowana - deklaracją zgodności, maksymalne obciążanie: do 800kg, - miejsce na panel wentylacyjny (4 wentylatory), - 2 x organizer pionowy na okablowanie, - 1x zamek drzwi przednich z klamką, - 1x zamek drzwi tylnych, - 2x zamek paneli bocznych,	

- 4x kółka transportowe (2 z hamulcem), - 4 nóżki poziomujące, 4. Macierz dyskowa musi być zainstalowana (dyski zamontowane) i skonfigurowana do pracy wg ustaleń z zamawiającym, wykonawca przeprowadzi szkolenie z obsługi macierzy. 5. Serwery oraz macierz muszą być zainstalowane i skonfigurowane, gotowe do pracy wg ustaleń z zamawiającym. W odniesieniu do serwera Wykonawca przeszkoli w zakresie obsługi i administracji serwera administratora sieci. Serwer ma umożliwiać między innymi archiwizację przyrostową i pełną serwerów zainstalowanych w budynku urzędu 6. Przeniesienie elementów aktywnych oraz struktury informatycznej z szafy rackowej nr 1 do szafy rackowej nr 2 z zachowaniem ciągłośći działania sieci i systemów teleinformatycznych 7. Doprowadzenie do każdego stanowiska komputerowego oraz urządzenia sieciowego osobnej linii dedykowanej przewodem UTP KAT. 6 zakończonej na patchpanelu w szafie rackowej w pomieszczeniu serwerowni. 8. Podłączenie kabli sieciowych do paneli krosowych oraz pomiar ciągłości wszystkich przewodów UTP -45 linii. 9. Opis wszystkich podłączonych i zakończonych elementów na patchpanelu. Przewody w korytach plastikowych zakończone przy urządzeniach gniazdami oraz podłączeniami przewodami patchcord do urządzeń 10. Wykonanie aktualnego schematu infrastruktury teleinformatycznej z rozpisaniem urządzeń aktywnych 11. Doposażenie pomieszczenia serwerowni w system monitoringu parametrów środowiskowych (czujnik dymu, czujnik temperatury) z uruchomioną funkją powiadamiania o parametrach na telefon. 12. Doposażenie, podłączenie w serwerowni oraz konfigurację kamery CCTV do istniejącego rejestratora monitoringu 13. Zamawiający dokona zainstalowania i skonfigurowania DC wraz z kontrolerem zapasowym DC - Utworzy i skonfiguruje role: WSUS, DHCP, SERWER PLIKÓW, NTP, - Przeprowadzi audyt istniejących polityk oraz wdroży rekomendowane polisy bezpieczeństwa, - Utworzy 3 przykładowe polityki GPO. - Uruchomi dodatkowe usługi – zgodnie z potrzebami Zamawiającego. - Przeprowadzi instruktaż dla Administratora. - Zainstaluje wszystkie zamówione programy, zaktualizuje do najnowszej wersji.. 14. Wdrożenie oprogramowania w zamówionego w powyższym przetargu na wszystkich komputerach. 15. Wdrożenie oprogramowania backupu. Zakres backupu systemów fizycznych oraz systemów wirtualnych.	

16. Listwy zasilające, montowane w uchwyty rack 19”. Podłączenie do źródła prądu 17. Rozbudowa rozdzielni o dodatkowe zabezpieczenie dla zasilania UPS w szafie serwerowej. 18. Doprowadzenie dedykowanego obwodu elektrycznego z rozdzielni do szafy serwerowej.	

Dotyczy urządzenia UTM

W przypadku istnienia wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Termin wykonania zamówienia.

Wykonanie zamówienia: Wykonawca zobowiązuje się do wykonania przedmiotu zamówienia w nieprzekraczalnym terminie do 2 miesięcy licząc od daty otrzymania zlecenia i jego akceptacji i/lub zawarcia umowy.

Wykonanie zamówienia

Urządzenia dostarczane w ramach przedmiotu zamówienia muszą być sprawne technicznie, nowe (nie starsze niż 1 rok licząc od momentu ogłoszenia zapytania ofertowego) i wolne od wad. Wykonawca zobowiązuje się do wykonania przedmiotu zamówienia w nieprzekraczalnym terminie do 6 miesięcy licząc od daty otrzymania zlecenia i jego akceptacji i/lub zawarcia umowy. Podczas prac należy zapewnić ciągłość działania infrastruktury teleinformatycznej. W pomieszczeniu serwerowni obecnie znajduje się główny punkt dystrybucyjny, wyposażony w przełączniki sieciowe, router, rejestrator monitoringu, UPS-y oraz jest to główny punkt gdzie schodzą się kable UTP, światłowody, przewody monitoringu. W związku z tym prace remontowe i instalacyjne muszą uwzględniać ciągłość działania sieci teleinformatycznej oraz płynne przejście ze starej infrastruktury teleinformatycznej na nową, zawartą w zapytaniu.

Dotyczy serwera:
Oferent winien przedłożyć oświadczenie producenta, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta oraz, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

Dotyczy jednostek komputerowych
Oferent winien przedłożyć oświadczenie producenta, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.