Bierzwnik, dnia 26.06.2023 r.

Znak sprawy: IS.VI.042.2.2.1.2022

ZAPYTANIE OFERTOWE

na realizację zamówienia w ramach

przedsięwzięcia grantowego pn.: *„Cyfrowa Gmina”*

objętego umową nr 3479/1/2021 o powierzenie grantu w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

I. ZAMAWIAJĄCY

Gmina Bierzwnik ul. Kopernika 2, 73-240 Bierzwnik NIP 5941534297, REGON 210967030, tel. 95 768 01 30/ fax. 95 768 01 11, e-mail: urzad@bierzwnik.pl, www.bierzwnik.pl

II. TRYB UDZIELANIA ZAMÓWIENIA PUBLICZNEGO

1. Postępowanie o udzielenie zamówienia publicznego prowadzone w trybie zapytania ofertowego, do którego nie stosuje się przepisów ustawy z dnia 11 września 2019 r - Prawo zamówień publicznych do zamówień publicznych na podstawie art. 2 ust 1 pkt 1 (t. j. Dz.U. 2022 r. poz. 1710 ze zm.), których wartość nie przekracza 130 000 zł netto.

III. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest zakup i dostawa sprzętu i oprogramowania w celu zwiększenia cyfryzacji instytucji samorządowej oraz jednostek podległych, a także zwiększenie cyberbezpieczeństwa w związku z realizacją przedsięwzięcia grantowego pn.: „**Cyfrowa Gmina**”.

Spis przedmiotu zamówienia:

1. Stacja robocza wraz z monitorem i niezbędnym oprogramowaniem (5 szt.)
2. Laptop wraz z niezbędnym oprogramowaniem (8 szt.)
3. Słuchawki z mikrofonem (15 szt.)
4. Urządzenie klasy UTM z 3 letnim wsparciem technicznym (1 szt.)
5. Serwer do backup'u wraz z oprogramowaniem. (1 szt.)
6. Oprogramowanie zarządzające infrastrukturą informatyczną (1 szt.)
7. Chmura obliczeniowa (1 szt.)

KODY CPV

Kod: 30214000-2 Stacje robocze
Kod: 30213100-6 Komputery przenośne
Kod: 32342100-3 Słuchawki
Kod: 48210000-3 Pakiety oprogramowania dla sieci
Kod: 48710000-8 Pakiety oprogramowania do kopii zapasowych i odzyskiwania

Kod: 48982000-5 Pakiety oprogramowania do zarządzania konfiguracją
Kod: 72317000-0 Usługi przechowywania danych

2. Przedmiot zamówienia został podzielony na **7 części (zadań).** Zamawiający przewiduje możliwość składania ofert częściowych. Wykonawca może złożyć ofertę na każdą z części zamówienia (tzn. złożyć ofertę na jedną lub więcej części zamówienia), przy czym każdy Wykonawca może złożyć tylko jedną ofertę sam lub jako partner w konsorcjum.

1) Zadanie 1- zakup wraz z dostawą Stacji roboczych wraz z monitorem i niezbędnym oprogramowaniem (5 szt.)

Komputer (5 szt.):	
Procesor	- obsługujący funkcje karty grafiki, - przynajmniej 6-rdzeniowy, 12-wątkowy o częstotliwości bazowej 2,6GHz (ale nie więcej niż 3,0 GHz) - TDP maksymalnie 65W, Litografia: 14nm - Osiągający w teście Passmark CPU Mark średni wynik przynajmniej 17000. Do oferty należy dołączyć wydruk ze strony: https://www.cpubenchmark.net/high_end_cpus.html lub http://www.cpubenchmark.net/mid_range_cpus.html - Model nie starszy niż z 2021 r.,
Płyta główna	- Współpracująca z oferowanym procesorem; - Chipset rekomendowany przez producenta procesora. Obsługująca pamięci typu DDR4. - Wymagane gniazda kart rozszerzeń i napędów: - 2 złącza pamięci DDR4 (obsługa minimum do 64GB RAM), - 1 złącze PCI-Express 3.0 x16, - 1 złącza PCI-Express x1, - 4 złącza SATA3, - 1 złącze m.2 Wymienione gniazda nie mogą być uzyskane w wyniku zastosowania konwerterów lub przejściówek.
Porty wejścia / wyjścia	Płyta główna musi posiadać następujące zewnętrzne gniazda wejścia/wyjścia na I/O: - 1 gniazdo PS/2 - 1 gniazdo D-SUB, - 1 gniazdo HDMI - 8 gniazd USB (w tym minimum 4 gniazd w standardzie USB 3.0, minimum 2 gniazda USB 3.0 wyprowadzone na panelu przednim), - 1 gniazdo LAN, - 3 gniazda Audio,
Pamięć RAM	min. 16GB DDR4

Dysk twardy	min. 512GB w technologii SSD Pci-e M.2
Dysk twardy 2	min. HDD 1TB 7200rpm
Napęd optyczny	DVD+/-RW
Karta Grafiki:	- Zintegrowana z procesorem - Posiadająca przynajmniej wyjścia HDMI, D-SUB - Wymagana obsługa DirectX co najmniej w wersji 12.
Karta dźwiękowa	- Zintegrowana z płytą główną, zgodna z High Definition Audio.
Karta sieciowa	- Interfejs wbudowany w płytę główną - minimum 1 x 10/100/1000 Mbps (RJ-45, Gigabit Ethernet).
Obudowa	- MiniTower, - 1 zewnętrzna zatoka na napęd 5,25” - Musi umożliwiać instalację przynajmniej 5 dysków twardych (w tym minimum trzech 3,5”) przy czym zatoka 5,25 pozostaje wykorzystana na montaż napędu optycznego. - Minimum 2 USB 3.0 + 2 USB 2.0 na panelu przednim. - Musi umożliwiać montaż pełnoprofilowych kart rozszerzeń i posiadać min. 4 wolnych slotów. - Obudowa ma umożliwiać instalację przynajmniej 2 wentylatorów systemowych, w tym minimum jednego w rozmiarze 120mm. - Zasilacz umieszczony w górnej części obudowy. - Obudowa trwale oznaczona logo producenta jednostki centralnej
Zasilanie	- Standard ATX, o mocy max 400W z aktywnym filtrem PFC o sprawności 85% - Przystosowany do pracy w sieci 230V, 50Hz.
Klawiatura	Klawiatura USB w układzie polski programisty
Mysz	Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) – tego samego producenta co klawiatura + podkładka pod mysz
System operacyjny	System operacyjny klasy PC nie wymagający aktywacji za pomocą telefonu lub Internetu, spełniający następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji: Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje,

	poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) Internetowa aktualizacja zapewniona w języku polskim; Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi) Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. Wbudowany system pomocy w języku polskim; Wdrażanie IPSEC oparte na politykach – wdrapanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;

	Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; Wsparcie dla Sun Java i .NET Framework 2.0 , 3.0 , 3.5 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; Graficzne środowisko instalacji i konfiguracji; Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; Możliwość przywracania plików systemowych; System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). Telefoniczne wsparcie techniczne w języku polskim w dni robocze od 8:00 do 17:00 zapewniony przez producenta lub dostawcę co najmniej przez 5 lat od chwili zakupu Na dysku twardym dedykowana partycja umożliwiająca szybkie odtworzenie fabrycznie skonfigurowanej wersji systemu (Recovery). Licencja systemu operacyjnego musi pochodzić z oficjalnego kanału dystrybucyjnego w Polsce, musi być nowa, a klucz nigdy wcześniej nie wykorzystywany ani aktywowany.

Gwarancja i Serwis	Gwarancja producenta 36 miesięcy w systemie door to door. Czas skutecznej naprawy uszkodzonego sprzętu max. 6 dni roboczych. W przypadku usterki dysku twardego pozostaje on u Zamawiającego. Serwis świadczony przez producenta sprzętu lub przez firmę posiadającą autoryzację producenta. Firma serwisowa świadcząca usługi serwisowe musi spełniać normę ISO 9001.
Dodatkowe wymagania:	- Deklaracja CE / UE. - Certyfikaty jakości producenta - ISO 9001, ISO 14001, 27001, 50001 - Głośność jednostki mierzona według normy ISO 9296/7779 ma wynosić maksymalnie 24 dB (praca w trybie IDLE). Test przeprowadzony na konfiguracji ofertowanej. Do oferty należy dołączyć raport z testów wykonanych przez niezależną jednostkę badawczą.

Monitor (5 szt.):	
Przekątna ekranu	min.23 - max.24 cale (szerokoekranowy 16:9)
Matryca	matowa, podświetlenie LED
Rozdzielczość nominalna	1920x1080
Kontrast	min. 3000:1
Jasność	min. 250 cd/m²
Czas reakcji plamki	max. 4 ms
Porty/złącza	1x DVI-D 24 pin i 1x HDMI
Wyposażenie	**wbudowane głośniki lub dołączane dedykowane przez producenta monitora do tego modelu, stanowiące integralną całość z monitorem**, kabel sygnałowy DVI lub HDMI umożliwiający połączenie z komputerami stacjonarnymi opisanymi w niniejszym OPZ
Certyfikaty	Wybrany Wykonawca zobowiązany jest przed podpisaniem umowy przedłożyć certyfikat: CE
Gwarancja	**Okres gwarancji: 36 miesięcy**
Oprogramowanie biurowe (5 szt.):	
Oprogramowanie biurowe	Licencja bezterminowa, obsługa makr Visual Basic, pełna kompatybilność z dokumentami DOCX, XLSX, PPTX, oraz zawierającego KLIENTA POCZTY kompatybilnego z powyższymi dokumentami. Zintegrowany pakiet aplikacji biurowych musi zawierać co najmniej: edytor tekstów, arkusz kalkulacyjny, narzędzie do przygotowywania i prowadzenia prezentacji, narzędzie do zarządzania

	informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), zainstalowanie na jednym komputerze produktów pochodzących od różnych producentów nie jest uznane za ofertę zintegrowanego pakietu. Pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet biurowy powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-19 – cena połączenia nie większa niż cena połączenia lokalnego. Pakiet musi mieć publicznie znany cykl życia przedstawiony przez producenta, dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa – co najmniej na 5 lat od daty zakupu. Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0). Pakiet aplikacji biurowych powinien obsługiwać formaty dokumentów wymienione w Krajowych Ramach Interoperacyjności. Pakiet aplikacji biurowych powinien prawidłowo współpracować z aplikacjami w modelu chmury obliczeniowej, w szczególności do pracy grupowej i synchronizacji danych. Rozpoznawanie sieci i ich ustawienia bezpieczeństwa, rozpoznawać automatycznie urządzenia peryferyjne działające w tej sieci (np. drukarki, tablice interaktywne) oraz łączyć się automatycznie. Nie dopuszcza się realizacji funkcji przez więcej niż jedno oprogramowanie.

2) <u>Zadanie 2- zakup z dostawą laptopów wraz z niezbędnym oprogramowaniem (8 szt.)</u>

Nazwa komponentu	**Wymagane <u>minimalne</u> parametry techniczne**
Procesor	Procesor osiągający w teście PassMark CPU Mark wynik min. **13 550 punktów** (wynik testu zaproponowanego procesora musi być opublikowany w zestawieniu CpuBenchmark – stanowiącym załącznik **procesory.pdf** w niniejszym postępowaniu. Wyniki testów na podstawie zestawienia publikowanego na stronie www.cpubenchmark.net z dnia 01 marca 2023 r.). **Model/typ/nazwę/producenta oferowanego procesora należy wpisać do oferty.**
Ekran	Matryca 15,6”, technologia LED, obsługiwana rozdzielczość: 1920x1080, matryca antyrefleksyjna lub matowa.
Pamięć RAM	**min. 8 GB z możliwością rozbudowy do 32 GB**

Dysk twardy	**min. 512 GB** w technologii SSD M.2 PCIe
Karta graficzna	zaprojektowana do pracy w urządzeniach przenośnych
Karta dźwiękowa	zaprojektowana do pracy w urządzeniach przenośnych. Wbudowane głośniki stereo
Karta sieciowa/łączność	10/100/1000 Ethernet RJ 45, WiFi 802.11 ac, Bluetooth min. 5.2
Porty/złącza	Wbudowane: port HDMI, min. 2 xUSB 3.0 typ A, 1x USB 3.1 typ C, port słuchawek i mikrofonu (dopuszczalny port combo), czytnik kart pamięci, czytnik linii papilarnych. **Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.**
Bateria	Bateria 3-komorowa Litowojonowa lub litowo-polimerowa. Pojemność min. 41 Wh
Wymagania dodatkowe	Zintegrowana z obudową kamera internetowa o rozdzielczości min. 720p HD - Podświetlana klawiatura - Torba dedykowana rozmiarem do przenoszenia zaoferowanego notebooka. - Klawiatura (układ US-QWERTY)
Waga	- Waga netto notebooka nie większa niż 1,75 kg
System operacyjny i oprogramowanie użytkowe	System operacyjny nie wymagający aktywacji za pomocą telefonu lub Internetu, spełniający następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji: Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) Internetowa aktualizacja zapewniona w języku polskim; Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;

	Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi) Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. Wbudowany system pomocy w języku polskim; Wdrażanie IPSEC oparte na politykach – wdrapanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; Wsparcie dla Sun Java i .NET Framework 2.0 , 3.0 , 3.5 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;

	Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; Graficzne środowisko instalacji i konfiguracji; Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; Możliwość przywracania plików systemowych; System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). Licencja systemu operacyjnego musi pochodzić z oficjalnego kanału dystrybucyjnego w Polsce, musi być nowa, a klucz nigdy wcześniej nie wykorzystywany ani aktywowany.
Certyfikaty i standardy	Wybrany Wykonawca zobowiązany jest przed podpisaniem umowy przedłożyć następujące certyfikaty: - Deklaracja zgodności CE
Bezpieczeństwo	Układ służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania (układ TPM). Zabezpieczenie to musi posiadać możliwość szyfrowania dokumentów przechowywanych na dysku twardym przy użyciu klucza.
Gwarancja	**36 miesięcy na miejscu u Klienta.**

Oprogramowanie biurowe (8 szt.):	
Oprogramowanie biurowe	Licencja bezterminowa, obsługa makr Visual Basic, pełna kompatybilność z dokumentami DOCX, XLSX, PPTX, oraz zawierającego KLIENTA POCZTY kompatybilnego z powyższymi dokumentami. Zintegrowany pakiet aplikacji biurowych musi zawierać co najmniej: edytor tekstów, arkusz kalkulacyjny, narzędzie do przygotowywania i

	prowadzenia prezentacji, narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), zainstalowanie na jednym komputerze produktów pochodzących od różnych producentów nie jest uznane za ofertę zintegrowanego pakietu. Pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet biurowy powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-19 – cena połączenia nie większa niż cena połączenia lokalnego. Pakiet musi mieć publicznie znany cykl życia przedstawiony przez producenta, dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa – co najmniej na 5 lat od daty zakupu. Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0). Pakiet aplikacji biurowych powinien obsługiwać formaty dokumentów wymienione w Krajowych Ramach Interoperacyjności. Pakiet aplikacji biurowych powinien prawidłowo współpracować z aplikacjami w modelu chmury obliczeniowej, w szczególności do pracy grupowej i synchronizacji danych. Rozpoznawanie sieci i ich ustawienia bezpieczeństwa, rozpoznawać automatycznie urządzenia peryferyjne działające w tej sieci (np. drukarki, tablice interaktywne) oraz łączyć się automatycznie. Nie dopuszcza się realizacji funkcji przez więcej niż jedno oprogramowanie.

3) Zadanie 3- Zakup z dostawą słuchawek z mikrofonem (15 szt.)

Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Przeznaczenie	Telefonia internetowa
Konstrukcja	Nauszne
Technologie	Redukcja szumów
Złącza	1x USB
Dźwięk	Stereo
Kontrola dźwięku	Regulacja głośności
Długość przewodu	2,4 m
Gwarancja	**Okres gwarancji: 24 miesiące**

4) Zadanie 4- Zakup z dostawą urządzenia klasy UTM z 3 letnim wsparciem technicznym (1 szt.)

Wymagania Ogólne
System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę 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 wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii
1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:
1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 5 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:
1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 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 protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. 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. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są 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.
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. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje 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 istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje 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.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).

- Obsługa protokołu Diffie-Hellman grup 19, 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
- 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.
- Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia 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 posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.

4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia 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).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.

Projekt „Cyfrowa Gmina" jest dofinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020

4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia 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. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Certyfikaty

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

b) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe AHB/SOS

a) System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy.

System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

- Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
- Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
- Doradztwo w zakresie konfiguracji.
- Zdalne wsparcie techniczne.
- Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
- Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
- Przygotowanie urządzenia do zdalnej konfiguracji.
- Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
- Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
- Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
- Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Wymagania powinny być potwierdzone dokumentami:

- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany 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.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

5) Zadanie 5- Zakup z dostawą serwer do backup'u wraz z oprogramowaniem. (1 szt.)

NAZWA PARAMETRU	WYMAGANIA MINIMALNE
Typ urządzenia	Serwer NAS
Obudowa	Tower
Procesor	Dwurdzeniowy procesor o taktowaniu 2.6 GHz (maksymalnie 3,1 GHz z przyspieszeniem) osiągający w teście PassMark w lutym 2023 co najmniej 3240 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	• Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 9 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej za pomocą portu eSATA • Wbudowane 2 gniazda M.2 obsługujące dyski NVMe. Dyski NVMe mogą posłużyć do utworzenia pamięć podręcznej bądź przestrzeni dyskowej Wbudowany slot 1x PCIe Gen3 x2 do podłączenia dodatkowej karty sieciowej 10GbE

Porty zewnętrzne	Minimum: - 2 porty USB 3.2.1 - 1 porty eSATA
Porty sieciowe	Minimum: 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Wentylator obudowy	Min. 2 wentylatory 92 mm x 92 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 128 • Minimalny liczba jednostek iSCSI LUN: 256 Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Ilość dysków zamontowanych	Min. 3 dyski SATA 6Gb/s, 256 MB cache, 5400RPM, o pojemności co najmniej 4TB każdy, znajdujących się na liście dysków kompatybilnych urządzenia, gwarancja 36 miesięcy, o współczynniku MTBF minimum 1 mln godzin.
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 1000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne

	blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane systemy klienckie	Windows® 7 i nowsze, macOS® 10.12 i nowsze
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz maks. 100 W
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić

	nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Gwarancja	**Wykonawca udzieli gwarancji:** **3 lat na urządzenia główne z możliwością przedłużenia do 5 lat za pomocą dodatkowego pakietu gwarancyjnego**

6) Zadanie 6- Zakup z dostawą oprogramowania zarządzającego infrastrukturą informatyczną (1 szt.)

NAZWA	WYMAGANIA MINIMALNE
Oprogramowanie zarządzające infrastrukturą informatyczną	**Wymagania ogólne dla systemu zarządzania:** System do profesjonalnego zarządzania zasobami IT. Wspierający i uzupełniający procesy strategicznego zarządzania przedsiębiorstwem zapewniając możliwość elastycznego i efektywnego rozwoju. Wybrane funkcjonalności zawarte w systemie: • W pełni webowa konsola zarzadzania systemem. • Baza danych pracująca na silniku Microsoft SQL Server • Wspólna baza CMDB dla całości systemu (infrastruktura, procesy, dokumenty, usługi, relacje). • System umożliwia wykorzystanie dowolnej liczby interfejsów sieciowych oraz wdrożenie architektury rozproszonej poprzez wykorzystanie wielu serwerów. • 100 interaktywnych widżetów. Widżety obsługują metodę drill-down i pozwala na pełną konfigurowalność. • Ponad 30 interaktywnych widgetów. Obsługa metody drill-down. Wskazuje elementy infrastruktury IT w obszarze bezpieczeństwa IT. • Spersonalizowany widok pod konkretnego użytkownika systemu (dashboardy, aktywne skróty). • Automatyczna inwentaryzacja infrastruktury IT w zakresie komputerów stacjonarnych i przenośnych, w sieci jak i poza siecią lokalną, a

	także serwerów, drukarek, dowolnych urządzeń sieciowych oraz zasobów dodanych manualnie. • Automatyczna inwentaryzacja systemów operacyjnych, oprogramowania zainstalowanego, oprogramowania portable. Wsparcie dla modeli: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value, CAL, SAAS, Trial, Shareware. • Zdalne zarządzanie komputerami – ponad 100 predefiniowanych poleceń CMD i PowerShell. • Zdalna instalacja, automatyczna zdalna instalacja / deinstalacja oprogramowania na jednym lub grupie komputerów. Wsparcie dla wielu repozytoriów. Automatyczny wybór repozytorium na podstawie wyznaczania optymalnej trasy pakietu. • Zdalne zarządzanie komputerami z wykorzystaniem RDP, VNC, Intel vPro. Zdalne połączenie do komputera w sieci lokalnej do sesji użytkownika. Multi VNC – jednoczesny dostęp do wielu komputerów. Pełne wsparcie dla technologii Intel VPRO/AMT w zakresie konfiguracji BIOS, uruchomienie wyłączonego komputera oraz reinstalację systemu operacyjnego • uruchomienie wyłączonego komputera oraz reinstalację systemu operacyjnego • automatyczne powiadomienia dotyczące aktualności w konsoli administracyjnej, (wspierane kanały: email, SMS, powiadomienia na pulpicie administratora, powiadomienia użytkownika), • zwracanie informacji o obciążeniu procesami, dyskach twardych oraz ruchu sieciowym • identyfikowanie sieci lokalnych oraz zbudowanie map sieci (w tym rozległych) oraz udostępnianie szczegółowych informacji o wszystkich urządzeniach sieciowych (obsługę SNMP) • Monitorowanie drukarek znajdujących się w sieci firmowej. Odczytywanie informacji szczegółowych o drukarkach (poziom tonerów, marginesy, powiadomienia, porty). Możliwość przejścia do panelu zarządzania drukarką. • Monitorowanie szybkości komunikacji między różnymi typami urządzeń dostępnych w infrastrukturze sieci a serwisami z których korzystają. • monitorowanie: logowania, drukowania, stron www, transferu sieciowego, urządzeń USB, usług, procesów, wydajności, dzienników zdarzeń, sesji RDP,

	• Monitorowanie procesów, usług oraz wydajności komputerów i serwerów (wspiera Hyper-V oraz VMware). Zwraca informację o obciążeniu procesami, dyskach twardych oraz ruchu sieciowym. • prowadzenie ewidencji ilościowo-wartościowej dla akcesoriów i infrastruktury informatycznej. • Klasyfikator stron internetowych / klasyfikator procesów i aplikacji - zaimplementowane klasyfikatory zwracają informację o kategorii, bezpieczeństwie oraz produktywności stron www i uruchamianych procesów / aplikacji, oparty o sztuczna inteligencja w zarządzaniu IT • zdalne wysyłanie alertów oraz jednorazowych lub cyklicznych wiadomości do użytkowników komputerów. Wiadomości podążają za użytkownikiem. • Możliwość komunikacji administratora IT z użytkownikami, w tym prowadzenie rozmów indywidualnych, grupowych, używanie harmonogramu, wiadomości predefiniowanych, statusy dostarczeni. • System powinien posiadać uwierzytelniania dwuskładnikowe, jest to dodatkowe zabezpieczenie poświadczeń użytkownika podczas procesu logowania. • System musi mieć uniwersalny interfejs programistyczny (API) do widoków tabelarycznych • System zapewnia monitorowanie zachowań użytkownika oraz grup użytkowników. Zakres monitorowania: logowanie, czas pracy, aktywność pracownika, uruchomiane procesy i aplikacje, wydruki, strony WWW, transfer sieciowy, używane urządzenia zewnętrzne USB. Obliczanie produktywności. • System pozwala na odczytywanie uprawnień do zasobów lokalnych i udostępnionych (lokalnych oraz sieciowych), możliwa dzięki zaimplementowanemu API. Monitorowanie 13 rodzajów uprawnień ACL (Access Control Lists). • System powinien posiadać panel pracownika - aplikacja webowa dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz umożliwiająca otrzymywanie kluczowych informacji w czasie rzeczywistym. W jednym miejscu możliwe jest proste oraz szybkie zgłaszanie problemów do działu wsparcia technicznego, odczytywanie komunikatów od administratorów sieci o planowanych przerwach w dostępie do usług, uczestnictwo w przypisanych szkoleniach z Learning

	• Kreator raportów, obsługa wysokowydajnych systemów raportujących. Umożliwia edytowanie ponad 200 predefiniowanych raportów oraz tworzenie nowych. Automatyczne generowanie raportów w wybranych formatach do kanałów: ścieżka UNC, e-mail, FTP.
	Standard raportów: SAP Business Objects oraz Stimulsoft (wersja web).
	• System wsparcia technicznego eHelpDesk Standard pomaga administratorom w obsłudze zgłoszeń problemów zgłoszonych przez użytkowników. Wybrane funkcjonalności zawarte w systemie:
	  • W pełni webowa konsola do zarzadzania systemem.
	  • Integracja z Active Directory
	  • Integralna cześć systemu do zarządzania zasobami IT tego samego producenta.
	  • Interfejs użytkownika umożliwia generowanie zgłoszeń serwisowych z poziomu formularza zgłoszeniowego oraz sprawdzanie statusu zgłoszeń w realizacji.
	  • Interfejs serwisanta umożliwia dokładną rejestrację i klasyfikację zgłoszeń oraz tworzenie dowolnych kategorii zgłoszenia.
	  • Zawiera pełną historię zgłoszenia.
	  • Możliwość automatycznego wysłania powiadomień e-mail o wszelkich zdarzeniach dotyczących zgłoszenia do zdefiniowanych użytkowników
	• Licencje bezterminowa na oprogramowanie musi objąć co najmniej 30 stanowisk komputerowych 12 miesięcznym wsparciem serwisowym.
	• Zdalne wykonanie instalacji, konfiguracji i profilowanie systemu
	• Minimum 2 godziny szkolenia z obsługi dostarczonego systemu
	• Certyfikat dla osób przeszkolonych

7) Zadanie 7- zakup wraz z dostawą chmury obliczeniowej (1 szt.)

L.P.	Parametr	Opis (minimalne wymagania)
1.	Licencja na oprogramowanie do tworzenia kopii zapasowej	Usługa kopii w chmurze **500GB z minimum roczną subskrypcją** Szyfrowanie przesyłu danych na linii komputer klienta – serwery w chmurze, przy wykorzystaniu protokołu SSL 256 bit. Szyfrowanie danych za pomocą algorytmu szyfrującego AES 256 bit. Dane szyfrowane są na komputerze użytkownika przy pomocy wygenerowanego wcześniej klucza szyfrującego, który przechowywany jest lokalnie u klienta. Nie ma możliwości odszyfrowania danych bez użycia niepowtarzalnego klucza będącego w posiadaniu jedynie użytkownika usługi. Rozwiązanie ma zapewniać pełną redundancję danych odporną na awarię dysków, węzłów, a nawet lokalizacji. Nowoczesne i certyfikowane (m.in. ISO/IEC 27001:2005) centrum danych spełniające najwyższe normy bezpieczeństwa pozwalające przechowywać dane na terenie Polski. Minimalny rozmiar dostępnego miejsca 500 GB 1. 15 użytkowników 2. backup baz danych bez limitu 3. backup plików i folderów 4. limit aktywnych linków – bez limitu 5. harmonogram zadań backupu 6. dostęp przez www, aplikacja desktop 7. własny klucz szyfrujący 8. szyfrowanie transmisji 9. wersjonowanie plików 10. synchronizacja danych 11. zaawansowane udostępnianie 12. powiadomienia email o statusie backupu 13. backup lokalizacji sieciowej

IV. TERMIN WYKONANIA ZAMÓWIENIA

Termin wykonania przedmiotu zamówienia do 10.07.2023 r.

V. PODSTAWY WYKLUCZENIA

1. Z udziału w postępowaniu ofertowym wykluczona się Wykonawców powiązanych z Gminą Bierzwnik osobowo lub kapitałowo. Powiązania osobowe lub kapitałowe oznaczają wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązańw imieniu Zamawiającego lub osobami wykonującymi w imieniu Gminy Bierzwnik czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru a Wykonawcą, polegające w szczególności na:

a) uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki osobowej,

b) posiadaniu co najmniej 10 % udziałów lub akcji, o ile najniższy próg nie wynika z przepisów prawa,

c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,

d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli. Wzór oświadczenia stanowi załącznik nr 2 zapytania ofertowego.

2. Z postępowania o udzielenie zamówienia Zamawiający wykluczy Wykonawcę w stosunku do którego zachodzi którakolwiek z okoliczności wskazanych w art. 7 ust 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowe (t.j. Dz. U. z 2023 r. poz. 129), tj.:

a) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3,

b) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 01 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 z późn. zm.) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającejo zastosowaniu środka, o którym mowa w art. 1 pkt 3,

c) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120 ze zm.) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisuna listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3.

VI. OPIS SPOSBU PRZYGOTOWANIA OFERTY

1. Wykonawcy ponoszą wszelkie koszty własne związane z przygotowaniem i złożeniem oferty, niezależnie od wyniku postępowania.
2. Oferta powinna być sporządzona na formularzu ofertowym stanowiącym **załącznik nr 1** do zapytania.
3. Oferta musi być sporządzona w języku polskim, w formie pisemnej, w sposób czytelny, na komputerze, maszynie lub pismem odręcznym.

4. Oferta oraz pozostałe dokumenty, dla których Zamawiający określił wzory w formie załączników, winny być sporządzone zgodnie z tymi wzorami co do treści. Wykonawca nie ma obowiązku załączenia wzoru umowy do składanej oferty.
5. Wykonawca składający dokumenty w innym języku niż język polski zobowiązany jest do złożenia ich wraz z tłumaczeniem na język polski, poświadczonym przez Wykonawcę.
6. Dokumenty sporządzone w języku obcym bez wymaganych tłumaczeń nie będą brane pod uwagę.
7. Oferta wraz z załącznikami musi być podpisana przez osoby upoważnione do składania oświadczeń woli w imieniu Wykonawcy. Jeżeli osoba podpisująca ofertę działa na podstawie pełnomocnictwa, to pełnomocnictwo to musi w swej treści jednoznacznie wskazywać uprawnienie do podpisania oferty. Pełnomocnictwo to musi zostać dołączone do oferty imusi być złożone w oryginale lub kopii poświadczonej za zgodność z oryginałem.
8. W przypadku gdy Wykonawca składa kopię jakiegoś dokumentu, musi być ona poświadczona za zgodność z oryginałem przez Wykonawcę.
9. Każdy Wykonawca składa tylko jedną ofertę, w jednym egzemplarzu.
10. Do oferty Wykonawca zobowiązany jest dołączyć aktualne na dzień składania ofert:

1) **Formularz Ofertowy** - wg **załącznika nr 1** do niniejszego Zapytania Ofertowego.

2) **Oświadczenie, że** wykonawca nie jest powiązany osobowo i kapitałowo z Gminą Bierzwnik - wg **załącznika nr 2** do niniejszego Zapytania Ofertowego.

3) Oświadczenie, że Wykonawca nie podlega wykluczeniu - wg **załącznika nr 3** do niniejszego Zapytania Ofertowego. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenia, o którym mowa powyżej składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenie to ma potwierdzać brak podstaw wykluczenia, w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.

4) **Klauzulę informacyjna RODO**, której wzór stanowi **załącznik nr 4** do niniejszego zapytania ofertowego.

VII. MIEJSCE ORAZ TERMIN SKŁADANIA OFERT

1. Ofertę należy złożyć w siedzibie Zamawiającego: Urząd Gminy Bierzwnik, ul. Kopernika 2, 73-240 Bierzwnik (sekretariat) **do dnia 04 lipca 2023 r. do godz. 8.30** poprzez platformę Baza Konkurencyjności, osobiście, kurierem, za pośrednictwem operatora pocztowego, e-mail na adres: urzad@bierzwnik.pl
lub za pośrednictwem skrzynki podawczej na platformie **E-PUAP.** Adres Elektronicznej Skrzynki Podawczej Zamawiającego **/t4khye646m/SkrytkaESP**. W przypadku składania ofert drogą elektroniczną należy złożyć skan podpisanego dokumentu lub dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym

lub podpisem osobistym. Za termin złożenia oferty przyjmuje się datę i godzinę wpływu oferty do Zamawiającego.

2. Oferty złożone po terminie nie będą rozpatrywane.

3. Ofertę wraz z wymaganymi dokumentami należy złożyć w zamkniętym opakowaniu opatrzonym napisem: Oferta na wykonanie zadania pn. ***„Cyfrowa Gmina"***, jeżeli będzie składana w formie innej niż drogą elektroniczną. Poza oznaczeniami powyżej na kopercie należy umieścić nazwę i adres Wykonawcy – dopuszcza się odcisk pieczęci z nazwą Wykonawcy.

4. Zamawiający nie przewiduje publicznego otwarcia ofert.

VIII. KRYTERIA OCENY OFERT

1. Zamawiający dokona oceny ofert na podstawie kryterium: **cena – 100%**.

2. Maksymalna łączna liczba punktów, jaką może uzyskać oferent za kryterium cena wynosi 100 pkt.

3. Punkty za kryterium cena zostaną obliczone według wzoru:

$$C = \frac{\text{cena najniższa spośród badanych ofert}}{\text{cena badanej oferty}} \times 100$$

C – liczba punktów, jakie otrzyma oferta za kryterium cena brutto przedmiotu zamówienia.

4. Przy obliczaniu punktów, Zamawiający zastosuje zaokrąglenie do dwóch miejsc po przecinku według zasady, że trzecia cyfra po przecinku od 5 w górę powoduje zaokrąglenie drugiej cyfry po przecinku w górę o 1. Jeśli trzecia cyfra po przecinku jest mniejsza niż 5, to druga cyfra po przecinku nie ulega zmianie.

5. Wykonawca określi cenę w walucie krajowej (w zł) wraz z należnym podatkiem VAT (cena brutto).

6. Cena oferty zgodnie art. 3 ust. 1 pkt 1 ustawy o cenach winna zawierać wszystkie koszty związane z obowiązkami przyszłego wykonawcy, niezbędne do zrealizowania zamówienia.

7. Cenę ofertową należy podać z dokładnością do dwóch miejsc po przecinku.

8. Przyjętą przez Zamawiającego formą wynagrodzenia Wykonawcy jest wynagrodzenie ryczałtowe.

9. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towaru i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej cenie podatek od towarów i usług , który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca

składając ofertę, informuje Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usług, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

10. Zamawiający nie przewiduje możliwości prowadzenia rozliczeń w walutach obcych.

11. Zamawiający wybierze ofertę, która uzyska największą liczbę punktów.

IX. SPOSÓB POROZUMIEWANIA SIĘ Z ZAMAWIAJĄCYM

1. Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawca przekazują pisemnie na adres: Urząd Gminy Bierzwnik, ul. Kopernika 2, 73-240 Bierzwnik lub środków komunikacji elektronicznej: urzad@bierzwnik.pl, **/t4khye646m/SkrytkaESP** w rozumieniu ustawy z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2020 r., poz. 344).
2. W korespondencji kierowanej do Zamawiającego Wykonawca winien posługiwać się numerem sprawy określonym w Zapytaniu Ofertowym.
3. Oświadczenia, wnioski, zawiadomienia oraz informacje przekazane za pomocą środków komunikacji elektronicznej uważa się za złożone w terminie, jeżeli ich treść dotarła do adresata tj. na serwer Zamawiającego, przed upływem terminu i została niezwłocznie potwierdzona.
4. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści Zapytania Ofertowego.
5. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert, zmienić treść Zapytania Ofertowego.
6. Wszelkie modyfikacje, uzupełnienia i ustalenia oraz zmiany, w tym terminów, jak również pytania wykonawców wraz z wyjaśnieniami stają się integralną częścią Zapytania Ofertowego i będą wiążące przy składaniu ofert.
7. Zamawiający nie przewiduje zorganizowania zebrania z wykonawcami.
8. Osobą uprawnioną do porozumiewania się z wykonawcami jest Dominika Szymoniak, tel. 784 355 159, e-mail: kadry@bierzwnik.pl, od poniedziałku do piątku w godz. od 7.30 do 15.30.

X. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca związany będzie złożoną ofertą przez okres 30 dni przyjmując, że pierwszym dniem związania ofertą jest dzień otwarcia ofert.
2. Wykonawca może przedłużyć termin związania ofertą na czas niezbędny do zawarcia umowy, samodzielnie lub na wniosek Zamawiającego.

XI. ZASTRZEŻENIA ZAMAWIAJĄCEGO

1. W toku badania i oceny ofert Zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert lub innych składanych dokumentów lub oświadczeń. Wykonawcy są zobowiązani do przedstawienia wyjaśnień w terminie

wskazanym przez Zamawiającego.

2. Zamawiający zastrzega sobie możliwość wezwania Wykonawcy do uzupełnienia oferty o brakujące dokumenty w terminie wyznaczonym przez Zamawiającego.

3. Zamawiający dopuszcza oferowanie materiałów lub rozwiązań równoważnych, pod warunkiem, że zagwarantują one wykonanie zamówienia w zgodzie z treścią zapytania ofertowego oraz zapewnią uzyskanie parametrów technicznych i użytkowych nie gorszych od założonych w wyżej wymienionych dokumentach. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji, na Wykonawcy ciąży obowiązek każdorazowego przedłożenia Zamawiającemu stosownych dokumentów, stwierdzających, że proponowane materiały, dostawy i technologia zamienne spełniają (nie są gorsze) warunki/parametry techniczne i użytkowe zawarte w dokumentacji postępowania. Obowiązek udowodnienia równoważności powiązań technicznych i użytkowych leży wyłącznie po stronie Wykonawcy. We wszystkich przypadkach wymagania techniczne mają pierwszeństwo przed standardami producenta.

XII. UNIEWAŻNIENIE POSTĘPOWANIA

1. Zamawiający unieważnia postępowanie o udzielenie zamówienia publicznego, w szczególności jeżeli:

a) nie złożono żadnej oferty niepodlegającej odrzuceniu,

b) cena najkorzystniejszej oferty lub oferta z najniższą ceną przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia, chyba, że Zamawiający może zwiększyć tę kwotę do ceny najkorzystniejszej oferty,

c) wystąpiły okoliczności powodujące, że prowadzenie Zapytania Ofertowego lub jego rozstrzygnięcie zakończone wyborem oferty nie leży w interesie Zamawiającego,

d) postępowanie obarczone jest niemożliwą do usunięcia wadą uniemożliwiającą zawarcie ważnej umowy w sprawie zamówienia publicznego.

2. Zamawiający zastrzega sobie uprawnienie do zamknięcia postępowania bez dokonywania wyboru oferty lub do unieważnienia postępowania bez podawania przyczyn na każdym jego etapie.

3. Wykonawcom nie przysługują żadne roszczenia względem Zmawiającego w przypadku skorzystania przez niego z któregokolwiek z uprawnień wskazanych w zdaniu poprzednim.

XIII. KLAUZULA INFORMACYJNA

W związku z realizacją wymogów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, zwane dalej RODO) - Dz.U.UE. z 2016 r., L 119, poz. 1, informujemy, że:

1) Administratorem Państwa danych osobowych jest: **Wójt Gminy Bierzwnik, ul. Kopernika 2, 73-240 Bierzwnik**

2) Jeśli ma Pani/Pan pytania dotyczące sposobu i zakresu przetwarzania danych osobowych, a także przysługujących uprawnień, może się Pani/Pan skontaktować z Inspektorem Ochrony Danych Osobowych pisemnie za pomocą adresu iod@bierzwnik.pl lub na adres administratora.

3) Pani/ Pana dane osobowe przewarzane będą na podstawie obowiązujących przepisów prawa, obowiązujących umów oraz na podstawie udzielonej zgody.

4) Pani/Pana dane osobowe przetwarzane są w celu wykonywania przez Gminę Bierzwnik ustawowych zadań publicznych realizowanych na podstawie obowiązujących przepisów prawa, realizacji umów zawartych z kontrahentami Gminy Bierzwnik, a w pozostałych przypadkach - wyłącznie na podstawie wcześniej udzielonej zgody w zakresie i celu określonym w treści zgody.

5) W związku z przetwarzaniem danych odbiorcami Pani / Pana danych osobowych mogą być:

a) organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i celach, które wynikają z przepisów powszechnie obowiązującego prawa,

b) inne podmioty, które na podstawie stosownych umów podpisanych z Gminą Bierzwnik przetwarzają dane osobowe dla których Administratorem jest Wójt Gminy Bierzwnik.

6) Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji celu dla jakiego zostały zebrane, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa.

7) Ma Pani/Pan prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych, prawo do żądania ich sprostowania (poprawienia), usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania.

8) Osoba, której dane przetwarzane są na podstawie zgody wyrażonej przez tę osobę (art. 6 ust. 1 lit. a RODO) ma prawo do cofnięcia tej zgody w dowolnym momencie. Cofnięcie to nie ma wpływu na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, z obowiązującym prawem.

9) Przysługuje Państwu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Państwa danych osobowych przez Administratora Danych. Organem właściwym dla skargi jest: Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa

10) W sytuacji, gdy przetwarzanie danych osobowych odbywa się na podstawie zgody osoby, której dane dotyczą, podanie przez Panią/Pana danych osobowych Administratorowi ma charakter dobrowolny.

11) Podanie danych osobowych jest obowiązkowe, w sytuacji gdy przesłankę przetwarzania danych osobowych stanowi przepis prawa lub zawarta między stronami umowa.

12) Pana/Pani dane nie będą przetwarzane w sposób zautomatyzowany i nie będą profilowane.

XIV. ZAŁĄCZNIKI DO ZAPYTANIA OFERTOWEGO

Załącznik nr 1 Formularz Ofertowy
Załącznik nr 2 Oświadczenia o braku powiązań osobowych i kapitałowych z Gminą Bierzwnik
Załącznik nr 3 Oświadczenie o braku podstaw wykluczenia
Załącznik nr 4 Klauzula informacyjna RODO
Załącznik nr 5 Wzór umowy

Zatwierdzam:
Wójt Gminy Bierzwnik
Aneta Kołuda

Aneta Maria Kołuda
Elektronicznie podpisany przez Aneta Maria Kołuda

Projekt „Cyfrowa Gmina" jest dofinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020