SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

RR.271.17.2022

w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie podstawowym opartym na wymaganiach wskazanych w art. 275 pkt. 1 ustawy Pzp.

o

dla zamówienia o nazwie:

**„Modernizacja sieci informatycznej w ramach projektu grantowego Cyfrowa Gmina”**

Link do postępowania: http://bip.starozreby.pl/wiadomosci/3/wiadomosc/657673/modernizacja\_sieci\_informatycznej\_w\_ramach\_projektu\_grantowego\_c

Identyfikator postępowania: ocds-148610-eda537d9-6407-11ed-abdb-a69c1593877c

Zatwierdzona przez:

/-/ Kamil Groszewski

## ROZDZIAŁ I. ZAMAWIAJĄCY (NAZWA I ADRES)

1. Gmina Staroźreby ul. Płocka 18

09-440 Staroźreby

NIP: 7743186342 ; REGON: 611016040 tel. 24 266 30 80 fax. 24 266 30 99

gmina@starozreby.pl

zwany dalej „Zamawiającym”.

1. Adres strony, na której dostępne będą dokumenty związane z zamówieniem, wyjaśnienia SWZ i wszelkie zmiany.

https://ezamowienia.gov.pl/pl/

Link do postępowania: http://bip.starozreby.pl/wiadomosci/3/wiadomosc/657673/modernizacja\_sieci\_informatycznej\_w\_ramach\_projektu\_grantowego\_c

## ROZDZIAŁ II. TRYB UDZIELENIA ZAMÓWIENA

Dotyczy części 1, 2, 3

1. Postępowanie prowadzone jest w trybie podstawowym opartym na wymaganiach wskazanych w art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2022 r. poz. 1710 ze zm. ) dalej: „ustawa Pzp” oraz aktów wykonawczych do tej ustawy.
2. W przypadku jakichkolwiek wątpliwości, niejasności, wykonawca winien przyjąć, że w pierwszej kolejności mają zastosowanie przepisy ustawy Pzp i aktów wykonawczych, a w drugiej kolejności zapisy niniejszej SWZ oraz treść ogłoszenia o zamówieniu.
3. Wykonawca jest zobowiązany zapoznać się z treścią niniejszego dokumentu i załączników. W przypadku uwag czy wątpliwości proszony jest o zasygnalizowanie ich przed terminem składania ofert. Szczegóły i zasady kontaktu i porozumiewania się z wykonawcami wskazuje między innymi rozdział VII niniejszej SWZ. Zamawiający po terminie składania ofert nie będzie miał możliwości zmiany zasad postępowania wskazanych w niniejszej SWZ.
4. Zamawiający nie przewiduje wyboru oferty najkorzystniejszej z możliwością prowadzenia negocjacji.

## ROZDZIAŁ III. NAZWA I OPIS PRZEDMIOTU ZAMÓWIENA

Dotyczy części 1, 2, 3

1. Przedmiotem zamówienia jest Dostawa sprzętu komputerowego dla gminy Staroźreby w ramach projektu grantowego Cyfrowa Gmina.
2. Zamawiający informuje, że zadanie jest finansowane ze środków Unii Europejskiej w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia.
3. Przedmiot zamówienia został podzielony na zadania części:

Część 1: Stacje robocze – 15 sztuk wraz z monitorami i oprogramowaniem, Tablety – 18 sztuk

Część 2: serwer – 1 sztuka

Część 3: Zakup i konfiguracja oprogramowania firewall

1. Szczegółowy opis przedmiotu zamówienia dla poszczególnych części :

**Opis przedmiotu zamówienia.**

**Część pierwsza postępowania.**

**Komputer typu desktop**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
| Typ | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |
| Wydajność | Oferowany komputer przenośny musi osiągać w teście wydajności :  SYSMARK 25 – wynik min. 1300 – test z przeprowadzonej konfiguracji załączyć do oferty na wezwanie Zamawiającego.  Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).  Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego. |
| Pamięć operacyjna RAM | 16GB DDR4 2666Mhz możliwość rozbudowy do min 64GB, min. 4 sloty na pamięć RAM. |
| Parametry pamięci masowej | Dysk SSD M.2 PCIe NVMe Class 35 o pojemności 256GB |
| Wydajność grafiki | Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem DirectX 12, OpenGL 4.5, pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana osiągająca w teście Sysmark25 Creativity co najmniej 1300 punktów - wyniki na wezwanie załączyć do oferty. |
| Wyposażenie multimedialne | Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. |
| Obudowa | Typu SFF z obsługą kart PCI Express o niskim profilu, możliwość instalacji minimum dwóch dysków 2,5” lub 3,5”. Obudowa fabrycznie przystosowana do pracy w orientacji pionowej i poziomej.  Suma wymiarów obudowy nie przekraczająca 80 cm.  Zasilacz o mocy max. 260W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 92% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%,  Wyposażona w min. 3 kieszenie z czego min. 2 szt. 5,25” (dopuszcza się zastosowanie jednej kieszeni 5,25” w wersji SLIM dla napędu optycznego),  1 szt. 3,5”.  Obudowa umożliwiająca montaż 3 dysków twardych 3,5” lub 2,5”  Obudowa musi umożliwiać bez narzędziowe otwarcie, demontaż dysków twardych (3,5” oraz 2,5”), napędu optycznego oraz kart rozszerzeń.  Obudowa musi być wyposażona w czujnik otwarcia. |
| Zgodność z systemami operacyjnymi i standardami | Oferowane modele komputerów muszą posiadać certyfikat producenta oferowanego systemu operacyjnego, potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym (załączyć wydruk ze strony producenta oprogramowania) |
| Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego  Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu bootowania, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System musi realizować funkcjonalności: sprawdzenie Master Boot Record na gotowość do uruchomienia oferowanego systemu operacyjnego, test procesora, test pamięci, test wentylatora dla procesora, test podłączonego wyświetlacza, test napędu optycznego, test portów USB, test dysku twardego, test podłączonych kabli, test podłączonego głośnika  Czujnik otwarcia obudowy musi zbierać logi i zapisywać je w BIOS |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu. |
| BIOS | BIOS zgodny ze specyfikacją UEFI  - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o:  - modelu komputera, PN  - numerze seryjnym,  - numerze inwentarzowym (AssetTag),  - MAC Adres karty sieciowej,  - 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:  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  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  - obsługa Bios za pomocą klawiatury i myszy  bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.  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 identyfikację 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 |
| Certyfikaty i standardy | * Urządzenia muszą być wyprodukowane zgodnie z normą ISO 9001 oraz ISO 50 001 ( certyfikaty załączyć do oferty) * 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 (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram * Certyfikat TCO dla oferowanego modelu – załączyć wydruk ze strony <http://tcodevelopment.com/> lub certyfikat TCO ( ze względu na częste zmiany na ww. stronie internetowej dopuszcza się wersję archiwalną) |
| Warunki gwarancji | 3-letnia gwarancja producenta.  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.  Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). |
| Wsparcie techniczne producenta | Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub oferenta.  Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony. |
| System operacyjny - w ofercie należy podać nazwę oprogramowania | Zainstalowany system operacyjny Windows 11 Professional lub równoważny  Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze  Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.  Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  Klucz licencyjny musi być przypisany do komputera i umożliwiać instalację systemu operacyjnego na podstawie nośnika lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.  Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające:  - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,  - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi  - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne  - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji  - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania)  - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku \*.xml  Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. |
| Oprogramowanie zabezpieczające serwer – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:  • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,  • wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,  • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)  Szyfrowanie danych:  • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną anyransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware.  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64 bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2. Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowania własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:  1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową  2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.  3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:  - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari  4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących  5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie  6. Portal zarządzający musi umożliwiać:  a) przegląd wybranych danych na podstawie konfigurowalnych widgetów  b) zablokowania możliwości zmiany konfiguracji widgetów  c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e) eksport wszystkich skanów podatności do pliku CSV  Backup i przywracanie danych  - Deduplikacja danych na źródle,  - Backup przyrostowy i różnicowy,  - Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,  - Backup danych lokalnych – plikowy oraz poczty Outlook,  - Backup otwartych plików (VSS),  - Filtr plików oraz folderów,  - Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),  - Wyłączanie komputera po wykonaniu backupu,  - Przywracanie danych do wskazanej lokalizacji,  - Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,  - Wyszukiwanie plików w repozytorium użytkownika,  Ustawienia  - Automatyczne logowanie,  - Zapamiętywanie danych logowania,  - Automatyczne uruchamianie programu przy starcie systemu,  - Ustawianie priorytetu dla procesu backupu,  - Zmiana klucza szyfrującego,  - Ustawienia przepustowości/zajętości pasma,  - Konfiguracja wydajności procesu backupu,  Bezpieczeństwo  - Zastępowanie nazwy pliku GUID-em,  - Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,  - Kompresja danych,  - Transmisja po bezpiecznym protokole TLS,  - Deklaracja klucza szyfrującego dane użytkownika,  - Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,  - Obliczanie sumy kontrolnej,  - Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.  WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS,Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji. |
| Wymagania dodatkowe | Wbudowany w obudowę porty (nie dopuszcza się stosowania przejściówek na zewnątrz obudowy):  - 1x VGA,  - 2x DP (dołączona przejściówka DP na HDMI)  - 5x USB 3.2 z przodu obudowy w tym min. 1xUSB typ-C  - 4x USB 3.2 z tyłu obudowy,  - port sieciowy RJ-45,  - port szeregowy RS-232  - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy  - niski profil PCIe 3.0 x16  - niski profil PCIe 3.0 x1  - niski profil PCIe 3.0 x16(x4)  - 2x slot M.2 w tym jeden wolny  Klawiatura USB w układzie polski programisty  Mysz optyczna USB z dwoma przyciskami oraz rolką  Wbudowana nagrywarka DVD +/-RW |

**Monitor do komputera typu desktop**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne monitora** |
|  | Typ ekranu | Ekran ciekłokrystaliczny z aktywną matrycą LED, IPS lub VA 23,8” |
|  | Jasność | 250 cd/m2 |
|  | Kontrast | 1000:1 |
|  | Kąty widzenia (pion/poziom) | 178/178 stopni |
|  | Czas reakcji matrycy | max 8 ms |
|  | Rozdzielczość maksymalna | 1920 x 1080 przy 60Hz |
|  | Wyświetlane kolory | 16.7 milionów |
|  | Zakres pochylenie monitora | +20°~-5° |
|  | Powłoka powierzchni ekranu | Antyodblaskowa |
|  | Podświetlenie | System podświetlenia LED |
|  | Zużycie energii | Typowo 25W, czuwanie mniej niż 0,5W |
|  | Bezpieczeństwo | Monitor musi być wyposażony w tzw. Kensington Slot |
|  | Waga | Maksymalnie 6 kg |
|  | Złącze | VGA (D-sub) - 1 szt.  HDMI - 2 szt. |
|  | Gwarancja | 3 lata gwarancji z czasem reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. |
|  | Inne | Odłączana stopa, VESA 100mm  Redukcja migotania (Flicker free)  Filtr światła niebieskiego  głośniki 2x2W |

# 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:
   1. Pełna polska wersja językowa interfejsu użytkownika.
   2. 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:
   1. Posiada kompletny i publicznie dostępny opis formatu.
   2. 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.

* 1. Pozwala zapisywać dokumenty w formacie XML.

1. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb Zamawiającego.
2. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
3. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim.
4. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   1. Edytor tekstów.
   2. Arkusz kalkulacyjny.
   3. Narzędzie do przygotowywania i prowadzenia prezentacji.
   4. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).
5. Edytor tekstów musi umożliwiać:
   1. 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.
   2. Wstawianie oraz formatowanie tabel.
   3. Wstawianie oraz formatowanie obiektów graficznych.
   4. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
   5. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
   6. Automatyczne tworzenie spisów treści.
   7. Formatowanie nagłówków i stopek stron.
   8. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
   9. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
   10. Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu.
   11. Wydruk dokumentów.
   12. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
   13. 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.
   14. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
   15. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
   16. Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
6. Arkusz kalkulacyjny musi umożliwiać:
   1. Tworzenie raportów tabelarycznych.
   2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
   3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML).
   5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
   6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
   7. Wyszukiwanie i zamianę danych.
   8. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
   9. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
   10. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
   11. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
   12. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
   13. 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.
   14. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
7. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
   1. Przygotowywanie prezentacji multimedialnych, które będą:
   2. Prezentowanie przy użyciu projektora multimedialnego.
   3. Drukowanie w formacie umożliwiającym robienie notatek.
   4. Zapisanie jako prezentacja tylko do odczytu.
   5. Nagrywanie narracji i dołączanie jej do prezentacji.
   6. Opatrywanie slajdów notatkami dla prezentera.
   7. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
   8. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
   9. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
   10. Możliwość tworzenia animacji obiektów i całych slajdów.
   11. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
   12. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010, 2013, 2016 i 2019.
8. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
   1. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
   2. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
   3. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
   4. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
   5. Automatyczne grupowanie wiadomości poczty o tym samym tytule.
   6. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
   7. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.
   8. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
   9. Zarządzanie kalendarzem.
   10. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.
   11. Przeglądanie kalendarza innych użytkowników.
   12. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.
   13. Zarządzanie listą zadań.
   14. Zlecanie zadań innym użytkownikom.
   15. Zarządzanie listą kontaktów.
   16. Udostępnianie listy kontaktów innym użytkownikom.
   17. Przeglądanie listy kontaktów innych użytkowników.
   18. Możliwość przesyłania kontaktów innym użytkowników.
   19. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

**Tablety - 18 szt.**

Tablet o parametrach nie gorszych niż:

Wyświetlacz: 10", 1920 x 1200 px, IPS

Pamięć wbudowana [GB]: 32

Wielkość pamięci RAM [GB]: 4

Komunikacja: Wi-Fi 802.11 a/b/g/n/ac, Bluetooth 4.2, Moduł GPS

Złącza: Złącze USB,

Gwarancja oferowanego sprzętu min. 24 miesięcy

**Część druga postępowania**

**Serwer plików i aplikacji 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Obudowa  1U  Obudowa serwerowa do montażu w szafie RACK 19" wraz z wysuwanymi szynami  dedykowanymi do tego urządzenia przez producenta serwera.  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  Obudowa powinna posiadać możliwość instalacji interfejsu NFC do połączenia z aplikacją zarządzającą serwerem na telefonie.  Aplikacja zarządzająca powinna być dostępna na Android i iOS  obudowa powinna posiadać dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera. |
| **Płyta główna** | Płyta główna obsługująca co najmniej  jeden procesor i co najmniej 4 sloty na pamięć  taktowaną przynajmniej z częstotliwością 3200MT/s  przy użyciu odpowiednich procesorów.  Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0 |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | Procesor typu skalowalnego posiadające co najmniej 8 rdzeni działający  co najmniej z częstotliwością 2.9GHz lub równoważny osiągający w teście Passmark dostępnym na stronie <https://www.cpubenchmark.net/> wynik nie mniejszy niż 18 000 pkt. |
| **RAM** | Min. 64GB DDR4 LRDIMM 3200MT/s. Płyta główna powinna obsługiwać do 128GB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Memory Health Check, Memory Page Retire |
| **Gniazda PCIe** | - minimum dwa sloty PCIe x16 generacji 4 |
| **Interfejsy sieciowe/FC/SAS** | Możliwość rozbudowy o dwa interfejsy sieciowe 10Gb Ethernet  Na płycie głównej powinna być zainstalowana dwuportowa karta sieciowa 1GB BT  Karta nie może zajmować slotu PCIe |
| **Dyski twarde** | Zainstalowane dyski min. 2x 600GB SAS 10k  Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwoscią konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmiejszenia ilości wnęk na dyski twarde.    Możliwość instalacji dwóch dysków hot-swap z możliwością konfiguracji RAID 1. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy PCI-E, możliwe konfiguracje poziomów RAID: 0,1,5,10. |
| **Wbudowane porty** | min. port USB 2.0 oraz port USB 3.0, port VGA, |
| **Video** | Zintegrowana karta graficzna |
| **Wentylatory** | Redundantne Hot-Plug |
| **Zasilacze** | Zasilacz Hot-Plug min 500W. |
| **Bezpieczeństwo** | Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  Moduł TPM 2.0 v3  Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera  Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |
| **Karta Zarządzania** | Możliwość zainstalowania niezależnej karty zarządzającej od zainstalowanego na serwerze systemu operacyjnego posiadającej dedykowany port RJ-45 Gigabit Ethernet umożliwiającej:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika * możliwość podmontowania zdalnych wirtualnych napędów * wirtualną konsolę z dostępem do myszy, klawiatury * wsparcie dla IPv6 * wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer * integracja z Active Directory * możliwość obsługi przez ośmiu administratorów jednocześnie * Wsparcie dla automatycznej rejestracji DNS * wsparcie dla LLDP * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość podłączenia lokalnego poprzez złącze RS-232. * możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. * Monitorowanie zużycia dysków SSD * możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, * Automatyczne zgłaszanie alertów do centrum serwisowego producenta * Automatyczne update firmware dla wszystkich komponentów serwera * Możliwość przywrócenia poprzednich wersji firmware * Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON * Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych * Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. * Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera * Serwer musi posiadać możliwość dostępu bezpośredniego 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 lub WIFI. |
| **System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania** | Microsoft Windows Server 2022 lub równoważny  Przez system równoważny do Microsoft Windows Server 2022 Zamawiający rozumie system spełniający następujące wymagania funkcjonalne:  1. Wspierający graficzny interfejs użytkownika umożliwiający jego obsługę przy pomocy klawiatury i myszy.  2. Zapewniający natywne wsparcie dla środowiska .NET Framework 4.8.  3. Zapewniający możliwości zarządzania komputerami oraz użytkownikami na poziomie funkcjonalności usługi katalogowej Active Directory.  4. System operacyjny musi wspierać pracę domenową.  5. System operacyjny musi posiadać obsługę zdalnego pulpitu zgodnego z protokołem RDP.  6. System operacyjny musi posiadać możliwość uruchomienia serwera DNS.  7. Licencja na system operacyjny zapewnia uruchomienie systemu operacyjnego w środowisku fizycznym i min. 1 środowiska wirtualnego za pomocą wbudowanego mechanizmy wirtualizacji, bez konieczności zakupu dodatkowych licencji.  8. Umożliwiający obsługę minimum 48 TB pamięci RAM.  9. Posiada wbudowaną zaporę sieciową (firewall) dla połączeń przychodzących i wychodzących z systemu.  10. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.  11. Zapewniający pełne wsparcie dla podzespołów zainstalowanych w zamawianym sprzęcie komputerowym (przy ew. wykorzystaniu sterowników od odpowiednich producentów podzespołów).  12. Licencja na system operacyjny musi być bez ograniczeń czasowych. |
| Oprogramowanie zabezpieczające serwer – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:  • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,  • wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,  • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)  Szyfrowanie danych:  • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną anyransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware.  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2. Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:  1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową  2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.  3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:  - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari  4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących  5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie  6. Portal zarządzający musi umożliwiać:  a) przegląd wybranych danych na podstawie konfigurowalnych widgetów  b) zablokowania możliwości zmiany konfiguracji widgetów  c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e) eksport wszystkich skanów podatności do pliku CSV  Backup i przywracanie danych  - Deduplikacja danych na źródle,  - Backup przyrostowy i różnicowy,  - Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,  - Backup danych lokalnych – plikowy oraz poczty Outlook,  - Backup otwartych plików (VSS),  - Filtr plików oraz folderów,  - Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),  - Wyłączanie komputera po wykonaniu backupu,  - Przywracanie danych do wskazanej lokalizacji,  - Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,  - Wyszukiwanie plików w repozytorium użytkownika,  Ustawienia  - Automatyczne logowanie,  - Zapamiętywanie danych logowania,  - Automatyczne uruchamianie programu przy starcie systemu,  - Ustawianie priorytetu dla procesu backupu,  - Zmiana klucza szyfrującego,  - Ustawienia przepustowości/zajętości pasma,  - Konfiguracja wydajności procesu backupu,  Bezpieczeństwo  - Zastępowanie nazwy pliku GUID-em,  - Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,  - Kompresja danych,  - Transmisja po bezpiecznym protokole TLS,  - Deklaracja klucza szyfrującego dane użytkownika,  - Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,  - Obliczanie sumy kontrolnej,  - Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.  WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS,Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji. |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001.  Serwer musi posiadać deklaracja CE.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub równoważny certyfikat producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019 x64, Microsoft Windows 2022 x64 . |
| **Normy Środowiskowe** | Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr *- Wykonawca złoży dokument potwierdzający spełnianie*wymogu*.* |
| **Warunki gwarancji** | 36 miesięcy gwarancji producenta z czterogodzinnym czasem reakcji od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu. |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

**Zasilacz awaryjny do serwera – 1 szt.**

|  |  |
| --- | --- |
| **Dane Ogólne** | |
| Typ | Online |
| Moc | 3000VA / 2700W |
| Współczynnik Mocy | 0.90 |
| **Wejście** | |
| Zakres Napięcia Wejściowego | 120-276 VAC Depends on Load Level |
| Max THDi | ≤5% |
| Input PF | ≥ 0.99 at full load |
| Zakres Częstotliwości | 45Hz - 55Hz or 54Hz - 66Hz |
| Częstotliwość (Synchronized Range) | 45Hz - 55Hz or 54Hz - 66Hz |
| **Wyjście** | |
| Nominalne Napięcie Wyjściowe | 208/220/230/240 VAC |
| Napięcie Sinusoidalne | Tak |
| THDv | ≤2% Full Linear Load; ≤5% Non-Linear Load |
| Regulacja Napięcia (Tryb Bat.) | ±1% |
| Frequency (Battery Mode) | ±0,2Hz |
| **Dane Techniczne** | |
| Load Crest Ratio | 3:1 |
| Transfer Time [AC to Battery] | 0ms |
| Transfer Time [Inverter to Bypass] | 0ms |
| Transfer Time [Inverter to ECO] | 1ms |
| Transfer Time [ECO to Inverter] | <10ms (7-8ms typical) |
| Bypass | Before UPS Power-on: Default “No” Change to “Yes” via display panel Overload und UPS Failure: Automatically transfer to bypass By Setting: Voltage Rang: 120-276V ± 3% |
| Generator support | Tak |
| Overload Capacity | 12s @102%-130%; 1.5s @130%-150%; 100ms @ >150% |
| External Battery Connection | Tak |
| Charger | 1.5A |
| Fan Logic | Always on, automatic speed control |
| LCD Indicators | UPS status, Load level, Battery level, Input/Output voltage, AC mode, battery mode, Bypass mode, fault conditions; LCD Display colour : Blue, red, red flashing (depends on UPS status), direction swappable (rack/tower) |
| **Wydajność** | |
| LINE mode full Load | 92.5% |
| BATTERY mode full Load | 87.0% |
| Energy Star compliance | Tak |
| **Baterie i czas podtrzymania** | |
| Baterie | 6x 12V/9Ah |
| DC Voltage | 6 x 12V |
| Recharge Time | 3h to 90% |
| Full Load Backup Time | 3min |
| Half Load Backup Time | 11min |
| **Komunikacja i wyjścia** | |
| IEC C13 Outlet | 8 |
| IEC C19 Outlet | 1 |
| Programmable Outlets | Tak |
| Wejście | C20 |
| Oprogramowanie | WinPower |
| USB port | Tak |
| Wsparcie dla HID | Tak |
| RS-232 Port | Tak |
| Port rozszerzeń | Tak, 1 |
| Dry Contacts | Tak |
| EPO Port | Tak |
| **Środowisko** | |
| Poziom hałasu | < 45dB |
| Temperatura | 0°C – 40°C |
| Wilgotność | 0% - 95% RH (non-condensing) |
| **Logistyka** | |
| Klasyfikacja IEC 62040-3 | VFI-SS-311 |
| Zawartość opakowanie | UPS, Manual, USB Cable, Input Power Cable, 2x IEC Cable, RS-232 Cable, Tower holder, Rack Ears, EPO Plug, Dry Contacts Plug |
| Języki instrukcji | EN/DE/FR/RU/PL |
| EAN | 4260074974423 |
| Szerokość | 438 mm |
| Wysokość | 86.5 mm |
| Głębokść | 608 mm |
| Waga | 28.6 kg |
| Karton - Szerokość | 590 mm |
| Karton - Wysokość | 236 mm |
| Karton - Głębokść | 790 mm |
| Karton - Waga | 31.2 kg |
| Pcs. per box | 1 |
| Pcs. per layer | 2 |
| Pcs. per pal | 16 |

**Urządzenie do wykonywania kopii bezpieczeństwa – 1 szt.**

|  |  |
| --- | --- |
| Procesor | AMD RyzenTM V1500B quad-core 2.2 GHz |
| Wbudowana pamięć RAM | 4 GB |
| Maks. wielkość pamięci | 32 GB |
| Rodzaj pamięci | DDR4 |
| Liczba obsadzonych gniazd pamięci | 1 |
| Liczba zainstalowanych dysków tw. | 2 ( 2 x 2 TB) |
| Maks. liczba dysków | 6 |
| Obsługa hot-swap dysków | Tak |
| RAID | Tak |
| Poziomy RAID | * 0 * 1 * 10 (1+0) * 5 * 6 |
| Architektura sieci | GigabitEthernet |
| Interfejs sieciowy | 4 x 10/100/1000 Mbit/s |
| Gniazda we/wy | * 2 x eSATA * 4 x RJ-45 LAN * 1 x USB 3.1 * 2 x USB 3.1 |
| Liczba wentylatorów | 2 |
| Wentylator | 9.2 cm |
| Obudowa | Tower |
| Waga | 5.1 kg |
| Wymiary | 166 x 282 x 243 mm |

**Część trzecia postępowania**

**Minimalne szczegółowe wymagania techniczne dla zapory UTM (firewall) – 1 szt.**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były realizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

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 3 administratorów do poszczególnych instancji systemu.

System musi wspierać 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 – 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.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum 10 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 20 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

**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 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 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 1,4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 630 Mbps.

**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. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego 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

**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.

1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
3. 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.

**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.

1. 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.

**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.

**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.

**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.

**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 uprawniająca 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.

**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.

**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.

**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.

**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.

1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
3. 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 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 dwuskładnikowego 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 Firewall 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.

**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.

**Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać 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: 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 36 miesięcy.

**Gwarancja oraz wsparcie**

1. System musi być objęty serwisem gwarancyjnym producenta przez okres min. 24 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.
2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji NSE8) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty. Zamawiający dopuszcza, aby usługę wsparcia świadczył autoryzowany dystrybutor oferowanego urządzenia, ale wtedy wraz z ofertą należy dostarczyć oświadczenie tego dystrybutora o gotowości świadczenia takiego wsparcia na rzecz Zamawiającego wraz z zakresem tego wsparcia.
3. Przedmiot zamówienia obejmuje dostawę, transport przedmiotowego sprzętu spełniającego wymagania opisane w SWZ .
4. Sprzęt wskazany powyżej musi być fabrycznie nowy, nieuszkodzony, wolny od wad fizycznych i wad prawnych.
5. Zamawiający nie dopuszcza oferowania sprzętu używanego lub po reaktywacji.
6. Sprzęt powinien być dostarczony Zamawiającemu w oryginalnych opakowaniach producenta wraz z dokumentami gwarancyjnymi i instrukcja obsługi w języku polskim.
7. Wykonawca zobowiązany jest do dostarczenia sprzętu, będącego przedmiotem zamówienia na własny koszt do siedziby Zamawiającego tj. do Urzędu Gminy w Staroźrebach ul. Płocka 18 09-440 Staroźreby w terminie 90 dni od podpisania umowy w sprawie zamówienia publicznego.
8. Zamawiający wymaga od Wykonawcy udzielenia min. 24 miesięcznej gwarancji na dostarczony sprzęt. Okres gwarancji będzie liczony od daty ostatecznego, bezusterkowego odbioru przedmiotu zamówienia.
9. Szczegółowy zakres przedmiotu zamówienia oraz wykaz asortymentu określa SWZ i załączniki.
10. Zamówienie obejmuje również dostawę z transportem (na koszt, ryzyko i odpowiedzialność Wykonawcy) sprzętu do siedziby Zamawiającego tj. 09-440 Staroźreby ul. Płocka 18 w dni robocze, od poniedziałku do piątku, w godzinach 9:00-14:00.
11. Za dostawę Zamawiający uważa: dowóz wyposażenia do miejsca wskazanego przez Zamawiającego, wniesienie wyposażenia i umiejscowienie w pomieszczeniu wskazanym przez Zamawiającego.
12. Do każdego urządzenia powinna zostać załączona instrukcja obsługi w języku polskim.
13. Wykonawca zobowiązany jest do wykonania zamówienia z najwyższą starannością, zgodnie z obowiązującymi przepisami, normami, zasadami wiedzy technicznej.
14. Za wypadki i szkody powstałe podczas realizacji zamówienia odpowiada Wykonawca.

Odpowiedzialność cywilną wobec osób trzecich jak i z tytułu zdarzeń losowych przyjmuje na siebie Wykonawca.

1. Dla sprzętu dostarczanego w ramach niniejszego zamówienia Zamawiający dopuszcza tolerancję wymiarów w zakresie +/-5% chyba, że w treści SWZ podany jest inny dopuszczalny zakres tolerancji.
2. Zamawiający, zgodnie z zapisami art. 99 ust. 5 i art. 101 ust. 4 ustawy Pzp, dopuszcza rozwiązania równoważne dla robót, materiałów, systemów spełniające obowiązujące standardy i wymagania. Zamawiający zastrzega, że wszędzie tam, gdzie w treści opisu przedmiotu zamówienia, stanowiącego opis przedmiotu zamówienia, zostały w opisie tego przedmiotu wskazane znaki towarowe, patenty lub pochodzenie urządzeń lub materiałów należy je traktować wyłącznie jako propozycje. Ponadto należy przyjąć, że wszystkim takim odniesieniom towarzyszą wyrazy "lub równoważne". Wskazanie równoważności oferowanego rozwiązania zgodnie z art. 101 ust. 5 ustawy i na zasadach tam określonych spoczywa na Wykonawcy. Zamawiający dopuszcza metody, materiały, urządzenia, systemy, technologie itp. równoważne do przedstawionych w opisie przedmiotu zamówienia. Dopuszcza się więc zaproponowanie w ofercie wszelkich równoważnych odpowiedników rynkowych o właściwościach nie gorszych niż wskazane przez Zamawiającego. Parametry wskazanego standardu określają minimalne warunki techniczne, eksploatacyjne, użytkowe, jakościowe i funkcjonalne, jakie ma spełniać przedmiot zamówienia. W ofercie można przyjąć metody, materiały, urządzenia, systemy, technologie itp. innych marek i producentów, jednak o parametrach technicznych, jakościowych i właściwościach użytkowych oraz funkcjonalnych odpowiadających metodom, materiałom, urządzeniom, systemom, technologiom itp. opisanym w SWZ. Na żądanie Zamawiającego, Wykonawca ma obowiązek udowodnienia, iż zastosowane rozwiązania równoważne pozwolą osiągnąć wszystkie założenia techniczne dla przedmiotu zamówienia, biorąc pod uwagę całość zadania, a nie wybrany fragment zadania. Ciężar udowodnienia, że materiał lub urządzenie jest równoważne w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy. Jeżeli materiały lub/i urządzenia zaoferowane przez Wykonawcę jako równoważne nie będą równoważne w świetle przedłożonych przez Wykonawcę dokumentów, oferta tego Wykonawcy zostanie odrzucona jako nieodpowiadająca treści SWZ. W przypadku zaś opisania przedmiotu zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, Zamawiający dopuszcza wykonanie zamówienia z zastosowaniem rozwiązań równoważnych opisywanym. Ponadto należy przyjąć, że wszystkim takim odniesieniom towarzyszą wyrazy "lub równoważne". W takim wypadku, procedurę opisaną na wstępie niniejszego punktu stosuje się odpowiednio. W przypadku opisu za pomocą norm za rozwiązania równoważne uznaje się takie rozwiązania, które zapewniają spełnienie wymagań minimalnych określonych w normie na poziomie nie gorszym niż opisano to w stosownych normach. W przypadku przywołanych w SWZ norm (jeżeli nie określono tego szczegółowo) rozumie się normy aktualne.
3. W przypadku przyjętych przez Wykonawcę do wyceny technologii, systemów, materiałów lub urządzeń równoważnych, do oferty musi być dołączony wykaz tych technologii, systemów, urządzeń lub materiałów, który będzie w swej treści zawierał podanie: rodzaj i opis zastosowanej technologii lub systemu, nazwy zastosowanego urządzenia/materiału, nazwy producenta, precyzyjnego i jednoznacznego typu urządzenia lub materiału.
4. Ponadto dla technologii/systemów/urządzeń/materiałów równoważnych Zamawiający wymaga udokumentowania równoważności, m.in. za pomocą załączonych do wykazu technologii/systemów/urządzeń/materiałów równoważnych; obliczeń, szczegółowych rysunków technicznych, atestów, aprobat, deklaracji zgodności przepisami i normami oraz kart katalogowych producentów urządzeń/materiałów równoważnych. Niniejsze dokumenty muszą w sposób jednoznaczny stwierdzać równoważność proponowanych technologii/systemów/urządzeń/materiałów.
5. W przypadku wątpliwości co do równoważności zaproponowanych w ofercie zamienników technologii/systemów/urządzeń/materiałów równoważnych, Zamawiający na etapie badania oferty może wymagać wykazania (udokumentowania) równoważności. W szczególności w tym celu może żądać przedstawienia przez Wykonawcę katalogów producenta danej technologii/systemów/urządzeń/materiałów równoważnych. W szczególności technologia/systemy/urządzenia/materiały równoważne oceniane będą pod względem możliwości uzyskania określonych dla technologii/systemów/urządzeń/materiałów poziomu funkcjonalności, kosztów eksploatacji, niezawodności działania.
6. Mając na uwadze treść art. 105 ustawy Pzp, Zamawiający podkreśla, iż nie ogranicza katalogu dokumentów jakie Wykonawca, w celu udowodnienia równoważności, winien przedłożyć w ofercie.
7. Jeżeli do oferty Wykonawcy nie zostanie załączony wykaz proponowanych technologii/systemów/urządzeń/materiałów równoważnych Zamawiający przyjmie, iż Wykonawca odstępuje od oferowania tego rodzaju technologii, systemów, urządzeń lub materiałów.
8. Wymagania jakościowe, o których mowa w art. 246 ust. 2 ustawy, Zamawiający szczegółowo opisał w opisie przedmiotu zamówienia i załącznikach do SWZ.
9. Zamówienie jest przeznaczone do użytku osób fizycznych, dlatego zgodnie z art. 100 ust. 1 ustawy Pzp, Zamawiający przy sporządzaniu opisu przedmiotu zamówienia uwzględnił wymagania w zakresie dostępności dla osób niepełnosprawnych.
10. Wymagania jakościowe, o których mowa w art. 246 ust. 2 ustawy, Zamawiający szczegółowo opisał w opisie przedmiotu zamówienia i załącznikach do SWZ.
11. Nazwy i kody Wspólnego Słownika Zamówień: (CPV):

|  |  |
| --- | --- |
| 30200000-1 | Urządzenia komputerowe |
| 33195100-4 | Monitory |
| 30213200-7 | Komputer tablet |
| 48000000-8 | Pakiety oprogramowania i systemy informatyczne |
| 48820000-2 | Serwery |
| 35100000-5 | Urządzenia awaryjne i zabezpieczające |
| 48710000-8 | Pakiety oprogramowania do kopii zapasowych i odzyskiwania |
| 32420000-3 | Urządzenia sieciowe |

## ROZDZIAŁ IV. TERMIN WYKONANIA

Dotyczy części 1, 2, 3,

Termin wykonania zamówienia 90 dni od dnia podpisania umowy.

## ROZDZIAŁ V. INFORMACJE O SPOSOBIE KOMUNIKACJI

Dotyczy części 1, 2, 3,

1. Komunikacja pomiędzy Zamawiającym a Wykonawcami odbywać się będzie wyłącznie przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2020 r. poz. 344) przy użyciu platformy E-zamówienia, który dostępny jest pod adresem https://ezamowienia.gov.pl/pl/, oraz poprzez pocztę elektroniczną adres e-mail: wojt@staroźreby.pl
2. Zamawiający nie przewiduje innego sposobu komunikacji z Wykonawcą poza środkami komunikacji elektronicznej.
3. Wykonawcy składający oferty za pośrednictwem ePUAP muszą posiadać konto firmy na ePUAP.
4. Na Platformie ePUAP będą dostępne dwa formularze dla Wykonawcy:

* Formularz do Komunikacji
* Formularz do złożenia, zmiany, wycofania oferty lub wniosku

1. Wymagania techniczne i organizacyjne wysyłania, składania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń zostały szczegółowo opisane w Instrukcji na portalu eZamówinia oraz w Warunkach korzystania z platformy administracji publicznej ePUAP.
2. Maksymalny rozmiar plików przesyłanych za pośrednictwem dostępnych na portalu e-Zamówinia formularzy wynosi 150 MB.
3. Wiadomości przekazywane droga elektroniczną powinny w sposób jednoznaczny wskazywać nr postępowania oraz dane identyfikujące wykonawcę.
4. Formaty plików muszą być zgodne z krajowymi Ramami Interoperacyjności ROZPORZĄDZENIE 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 (Dz.U. z 2017r. poz.2247). Zamawiający nie dopuszcza przesyłania plików w następujących formatach:
   1. - .com
   2. - .exe 3) - .bat

4) - .msi.

1. Za datę przekazania oferty, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich przekazania na ePUAP.
2. Każda oferta musi być zaszyfrowana. Zaszyfrowane oferty stanowią załącznik do przesłanego na ESP wniosku.
3. Ofertę należy złożyć w języku polskim.
4. Ofertę składa się pod rygorem nieważności w formie elektronicznej lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym poświadczając zgodność odzwierciedlenia cyfrowego z oryginałem dokumentów w postaci papierowej. 13. Zamawiający dopuszcza dołączenie do oferty katalogu elektronicznego
5. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa” a następnie wraz z plikami stanowiącymi jawną część należy ten plik zaszyfrować.
6. Do oferty należy dołączyć oświadczenie o niepodleganiu wykluczeniu, spełnianiu warunków udziału w postępowaniu lub kryteriów selekcji, wszystkie dokumenty wskazane w SWZ, w formie elektronicznej

lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym, a następnie zaszyfrować wraz z plikami stanowiącymi ofertę.

1. Osobą do kontaktu i porozumiewania się z wykonawcami jest: 1) w sprawach dotyczących przedmiotu zamówienia:
   1. Justyna Wilamowska tel. 24 266 30 95, e-mail: [zamowieniapubliczne@starozreby.pl](mailto:zamowieniapubliczne@starozreby.pl)
   2. Kamil Groszewski tel. 24 266 30 81 , e-mail: [wojt@starozreby.pl](mailto:wojt@starozreby.pl)
2. Zamawiający nie przewiduje: 1) wizji lokalnej,

2) zebrania wykonawców.

## ROZDZIAŁ VI. TERMIN ZWIĄZANIA OFERTĄ

Dotyczy części 1, 2, 3,

Termin związania ofertą: 30 dni t.j. od 24 listopada i do dnia 24 grudnia 2022r. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert, dzień ten jest pierwszym dniem terminu związania ofertą.

## ROZDZIAŁ VII. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

Dotyczy części 1, 2, 3,

1. Wykonawca może złożyć tylko jedną ofertę.
2. Treść oferty musi odpowiadać treści SWZ.
3. Ofertę należy sporządzić na formularzu oferty lub według takiego samego schematu, stanowiącego załącznik nr 1 do SWZ. Ofertę należy złożyć pod rygorem nieważności w formie elektronicznej lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
4. Wraz z ofertą wykonawca jest zobowiązany złożyć:
   1. oświadczenie o niepodleganiu wykluczeniu, spełnianiu warunków udziału w postępowaniu, w zakresie wskazanym przez zamawiającego (załącznik nr 2 do SWZ), aktualne na dzień składania ofert.
   2. Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej (załącznik nr 7 do SWZ),
   3. W przypadku wspólnego ubiegania się o zamówienie przez wielu wykonawców, oświadczenie, o którym mowa powyżej, składa każdy z wykonawców.

Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.

* 1. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu lub kryteriów selekcji, w zakresie, w jakim wykonawca powołuje się na jego zasoby.
  2. Zobowiązanie podmiotu udostępniającego zasoby do oddania wykonawcy do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
  3. Pełnomocnictwo ustanowione do reprezentowania Wykonawcy/ów ubiegającego/cych się o udzielenie zamówienia publicznego.
  4. Przedmiotowe środki dowodowa o których mowa w rozdziale XV SWZ (jeżeli są wymagane).
  5. Dowód wniesienia wadium (jeżeli jest wymagane).
  6. Oświadczenie w związku z art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego nie podlega wykluczeniu w związku z art. 7 ust.1 ustawy z dnia 13 kwietnia 2022r. – załącznik nr 7 do swz.

1. Oferta powinna być podpisana przez osobę upoważnioną do reprezentowania wykonawcy, zgodnie z formą reprezentacji wykonawcy określoną w rejestrze lub innym dokumencie, właściwym dla danej formy organizacyjnej wykonawcy albo przez upełnomocnionego przedstawiciela wykonawcy. W celu potwierdzenia, że osoba działająca w imieniu wykonawcy jest umocowana do jego reprezentowania, Zamawiający żąda od wykonawcy odpisu lub informacji z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru,
2. Oferta oraz pozostałe oświadczenia i dokumenty, dla których Zamawiający określił wzory w formie formularzy zamieszczonych w załącznikach do SWZ, powinny być sporządzone zgodnie z tymi wzorami, co do treści oraz opisu kolumn i wierszy.
3. Ofertę składa się pod rygorem nieważności w formie elektronicznej lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
4. Oferta powinna być sporządzona w języku polskim. Każdy dokument składający się na ofertę powinien być czytelny.
5. Jeśli oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Wykonawca powinien nie później niż w terminie składania ofert, zastrzec, że nie mogą one być udostępnione oraz wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa .Przed upływem terminu składania ofert, wykonawca może wprowadzić zmiany do złożonej oferty lub wycofać ofertę. W tym celu należy w systemie Platformy kliknąć przycisk „Wycofaj ofertę”. Zmiana oferty następuje poprzez wycofanie oferty oraz jej ponowne złożenie. Podmiotowe środki dowodowe lub inne dokumenty, w tym dokumenty potwierdzające umocowanie do reprezentowania, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.
6. Wszystkie koszty związane z uczestnictwem w postępowaniu, w szczególności z przygotowaniem i złożeniem oferty ponosi wykonawca składający ofertę. zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

## ROZDZIAŁ VIII. SPOSÓB I TERMIN SKŁADANIA OFERT

Dotyczy części 1, 2, 3,

1. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do następujących formularzy: „Formularz do złożenia, zmiany, wycofania oferty lub wniosku” oraz do „Formularza do komunikacji”.
2. Za datę przekazania oferty, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich przekazania na ePUAP.
3. Zamawiający przekazuje link do postępowania oraz ID postępowania.
4. Dane postępowanie można wyszukać również na Liście wszystkich postępowań w portalu e-Zamówienia klikając wcześniej opcję „Dla Wykonawców” lub ze strony głównej z zakładki Postępowania.
5. Wykonawca składa Ofertę o dopuszczenie do udziału w postępowaniu, dalej „wniosek” za pośrednictwem „Formularza do złożenia, zmiany, wycofania oferty lub wniosku” dostępnego na eZamówienia.
6. W formularzu oferty/wniosku wykonawca zobowiązany jest podać adres skrzynki ePUAP, na którym prowadzona będzie korespondencja związana z postępowaniem lub adres e-mail.
7. Ustala się termin składania ofert na dzień 24 listopada 2022 r., godz. 12:00.
8. Za datę i godzinę złożenia oferty rozumie się datę i godzinę jej wpływu na portalu e-Zamówinia.
9. W przypadku otrzymania przez Zamawiającego oferty po terminie podanym w ust. 8 niniejszego rozdziału SWZ, oferta zostanie odrzucona.

## ROZDZIAŁ IX. TERMIN OTWARCIA OFERT

Dotyczy części 1, 2, 3,

1. Otwarcie ofert nastąpi w dniu 24 listopada 2022 r., godz.12:05.
2. Najpóźniej przed otwarciem ofert, Zamawiający udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie niniejszego zamówienia (kwota brutto, wraz z podatkiem VAT).
3. Niezwłocznie po otwarciu ofert zamawiający udostępni na stronie internetowej prowadzonego postępowania informacje o nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte oraz cenach zawartych w ofertach.

## ROZDIAŁ X. PODSTAWY WYKLUCZENIA

Dotyczy części 1, 2, 3,

1. Na podstawie art. 108 ust. 1 ustawy PZP z postępowania o udzielenie zamówienia wyklucza się Wykonawcę:
   1. będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
      1. udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
      2. handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
      3. o którym mowa w art. 228-230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie lub w art. 54 ust. 1-4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2021 r. poz. 523, 1292, 1559 i 2054),
      4. finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
      5. o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
      6. powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769 oraz z

2020 r., poz. 2023),

* + 1. przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
    2. o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

- lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

* 1. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowoakcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;
  2. wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub

grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

* 1. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
  2. jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;
  3. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

1. Na podstawie art. 109 ust. 1 ustawy PZP wyklucza się Wykonawcę, który:
   1. naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
   2. w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;
   3. który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub kryteria selekcji, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych podmiotowych środków dowodowych;
   4. który bezprawnie wpływał lub próbował wpływać na czynności zamawiającego lub próbował pozyskać lub pozyskał informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;
   5. który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia.
2. Na podstawie art. 7ust. 1 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2022r. poz. 835), wyklucza się Wykonawcę, który:
   1. jest wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ww ustawy;
   2. beneficjentem rzeczywistym Wykonawcy w rozumieniu ustawy z dnia 1 marca 2018r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 poz. 593 i 655) 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 2022r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ww ustawy;
   3. jednostką dominującą Wykonawcy w rozumieniu art. 3 ust. 1 pkt. 37 ustawy z dnia 29 września 1994r. o rachunkowości (t.j. Dz. U. z 2021r. poz.. 217 z późn. 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 2022r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ww ustawy

## ROZDZIAŁ XI. WARUNKI UDZIAŁU W POSTEPOWANIU

Dotyczy części 1, 2, 3,

Na podstawie art. 112 ust. 2 o udzielenie niniejszego zamówienia publicznego mogą ubiegać się Wykonawcy, którzy spełniają warunki udziału w postępowaniu, dotyczące:

1. zdolności do występowania w obrocie gospodarczym; 1) Zamawiający nie określa tego warunku.

1. uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów;

1) Zamawiający nie określa tego warunku.

1. sytuacji ekonomicznej lub finansowej;

1) Zamawiający nie określa tego warunku.

1. doświadczenia zawodowego;

1) Wykonawca posiada doświadczenie polegające na dostawie sprzętu komputerowego tj. co najmniej 1 sztuki urządzenia w zależności od danej części wykazać w/w doświadczenie na załączniku nr 6 do swz.

[wykazu dostaw lub usług wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy lub usługi zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy lub usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy lub usługi zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy]

5.w zakresie osób zdolnych do wykonania zamówienia;

1) Zamawiający nie określa warunku udziału w postępowaniu w tym zakresie;

## ROZDZIAŁ XII. KORZYSTANIE Z ZASOBÓW INNYCH PODMIOTÓW W CELU POTWIERDZENIA SPELNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Dotyczy części 1, 2, 3,

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postepowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych innych podmiotów (dot. Warunków udziału w postępowaniu określonych przez Zamawiającego w rozdziale XI SWZ), niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
2. Wykonawca korzystający z zasobów innych podmiotów dołącza do oferty zobowiązanie podmiotu trzeciego – załącznik nr 7.
3. Na podstawie art. 125 ust. 5 wykonawca dołącza do oferty oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw do wykluczenia tego podmiotu – załącznik nr 2.
4. Wykonawca, który polega na zdolnościach innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia – dokument ten (np. zobowiązanie) należy dołączyć do oferty.

Z dokumentu (np. zobowiązania), o którym mowa w pkt 2 musi wynikać w szczególności:

* zakres dostępnych Wykonawcy zasobów innego podmiotu,
* sposób wykorzystania zasobów innego podmiotu, przez Wykonawcę, przy wykonywaniu zamówienia publicznego,
* zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego,
* czy podmiot, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane, których wskazane zdolności dotyczą.

1. Zamawiający ocenia, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 108 ustawy Pzp
2. Jeżeli zdolności techniczne lub zawodowe, podmiotu, o którym mowa powyżej, nie potwierdzają spełnienia przez Wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tych podmiotów podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego:
   1. zastąpił ten podmiot innym podmiotem lub podmiotami lub
   2. zobowiązał się do osobistego wykonania odpowiedniej części zamówienia, jeżeli wykaże zdolności techniczne lub zawodowe lub sytuację finansową lub ekonomiczną, o których mowa w pkt 1 niniejszego rozdziału.
3. Jeżeli Wykonawca wykazując spełnianie warunków udziału w postępowaniu, określonych przez Zamawiającego w pkt 4 rozdziału XI SWZ, polega na zdolnościach innych podmiotów, na zasadach określonych powyżej, zamieszcza informacje o tych podmiotach w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy.
4. Wykonawca zobowiązany będzie również złożyć wskazane w SWZ dokumenty tego podmiotu potwierdzające spełnianie warunków udziału w postępowaniu w zakresie zdolności, na których Wykonawca polegał w celu wykazania spełniania tych warunków.
5. Zamawiający nie określa zakresu zadań kluczowych do osobistego wykonania przez poszczególnych wykonawców w razie wspólnego ubiegania się o udzielenia zamówienia

## ROZDZIAL XIII. INFORMACJA NA TEMAT MOZLIWOŚCI SKŁADANIA OFERTY WSPÓLNEJ (PRZEZ DWA LUB WIĘCEJ PODMIOTÓW)

Dotyczy części 1, 2, 3,

1. Wykonawcy wspólnie ubiegający się o zamówienie muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego – nie dotyczy spółki cywilnej, o ile upoważnienie/pełnomocnictwo do występowania w imieniu tej spółki wynika z dołączonej do oferty umowy spółki bądź wszyscy wspólnicy podpiszą ofertę.
2. Wykonawcy tworzący jeden podmiot przedłożą wraz z ofertą stosowne pełnomocnictwo –– nie dotyczy spółki cywilnej, o ile upoważnienie/pełnomocnictwo do występowania w imieniu tej spółki wynika z dołączonej do oferty umowy spółki bądź wszyscy wspólnicy podpiszą ofertę.

Uwaga: Pełnomocnictwo, o którym mowa powyżej może wynikać albo z dokumentu pod taką samą nazwą, albo z umowy podmiotów składających wspólnie ofertę.

1. Oferta musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich Wykonawców występujących wspólnie (przez każdego z Wykonawców lub pełnomocnika).
2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie, o którym mowa w art. 125 ust.1 ustawy (załącznik nr 2) składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenia te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu, oraz brak podstaw wykluczenia (każdy z Wykonawców wspólnie składających ofertę nie może podlegać wykluczeniu z postępowania co oznacza, iż oświadczenie w tym zakresie musi złożyć każdy z Wykonawców składających ofertę wspólną; oświadczenie o spełnianiu warunków udziału składa podmiot, który w odniesieniu do danego warunku udziału w postępowaniu potwierdza jego spełnianie; dopuszcza się złożenie oświadczenia łącznie, pod warunkiem, iż oświadczenie to zostanie podpisane w imieniu wszystkich podmiotów występujących wspólnie (przez Pełnomocnika) lub wszystkie podmioty składające ofertę wspólną).
3. Dopuszcza się, aby wadium zostało wniesione przez pełnomocnika (lidera) lub jednego z Wykonawców wspólnie składających ofertę.
4. Wszelka korespondencja prowadzona będzie wyłącznie z podmiotem występującym, jako pełnomocnik Wykonawców składających wspólną ofertę.
5. Zamawiający może badać, czy nie zachodzą wobec podwykonawcy niebędącego podmiotem udostępniającym zasoby, podstawy wykluczenia, o których mowa w art. 108 i art. 109 ustawy Pzp.

ROZDZIAŁ XIV. INFORMACJA NA TEMAT PODWYKONAWCÓW

Dotyczy części 1, 2, 3,

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy.
2. Wykonawca, który zamierza wykonywać zamówienie przy udziale podwykonawcy, musi wyraźnie w ofercie wskazać, jaką część (zakres zamówienia) wykonywać będzie w jego imieniu podwykonawca oraz podać firmę podwykonawcy (z zastrzeżeniem pkt 3 niniejszego rozdziału). Należy w tym celu wypełnić odpowiedni punkt formularza ofertowego, stanowiącego załącznik nr 1 do SWZ.W przypadku, gdy Wykonawca nie zamierza wykonywać zamówienia przy udziale podwykonawców, należy wpisać w formularzu „nie dotyczy” lub inne podobne sformułowanie. Jeżeli Wykonawca zostawi ten punkt niewypełniony (puste pole) Zamawiający uzna iż zamówienie zostanie wykonane siłami własnymi, tj. bez udziału podwykonawców.
3. Wykonawca zobowiązany jest do zawiadamiania Zamawiającego o wszelkich zmianach w zakresie podwykonawców. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 118 ust. 1 ustawy, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu, że proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia. Nowy podwykonawca, który jednocześnie przekazuje swoje zasoby w celu wykazania spełniania warunków, nie może także podlegać wykluczeniu z postępowania w takim samym zakresie, jak Wykonawca.
4. Zamawiający żąda, aby przed przystąpieniem do wykonania zamówienia Wykonawca, o ile są już znane, podał nazwy albo imiona i nazwiska oraz dane kontaktowe podwykonawców i osób do kontaktu z nimi, zaangażowanych w wykonanie zamówienia. Wykonawca zobowiązany jest do zawiadomienia Zamawiającego o wszelkich zmianach danych, o których mowa w zdaniu pierwszym, w trakcie realizacji zamówienia, a także przekazuje informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację zamówienia.
5. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.

## ROZDZIAŁ XV. PODMIOTOWE ŚRODKI DOWODOWE

Dotyczy części 1, 2, 3,

W postepowaniu o udzielenie zamówienia Zamawiający żąda złożenia podmiotowych środków dowodowych na wezwanie Zamawiającego przez Wykonawcę, którego oferta została najwyżej oceniona, dotyczących:

1. braku podstaw wykluczenia:
   1. oświadczenie, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne i zdrowotne do Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego w zakresie art. 109 ust. 1 pkt.1;
   2. oświadczenie, że wykonawca nie zalega z opłacaniem podatków i opłat do Urzędu Skarbowego w zakresie art. 109 ust. 1 pkt 1:
   3. oświadczenie w zakresie art. 109 ust.1 pkt. 8,9,10
   4. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie w zakresie ust. 1 składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.
2. spełnienia warunków udziału w postepowaniu:
   1. wykaz dostaw sprzętu komputerowego tj. co najmniej 1 sztuki urządzenia w zależności od danej części wykazać w/w doświadczenie na załączniku nr 6 do swz.

[wykazu dostaw lub usług wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy lub usługi zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy lub usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy lub usługi zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy]

1. Oświadczenia i podmiotowe środki dowodowe Wykonawca składa w formie elektronicznej, w postaci elektronicznej opatrzonej podpisem kwalifikowanym, zaufanym lub osobistym.

## ROZDZIAŁ XVI. WYMAGANIA W ZAKRESIE ZATRUDNIENIA NA PODSTAWIE STOSUNKU PRACY, W OKOLICZNOŚCIACH, O KTÓRYCH MOWA W ART. 95

Dotyczy części 1, 2, 3,

Zamawiający nie określa tych wymagań.

ROZDZIAŁ XVII. INFORMACJA NA TEMAT CZĘŚCI ZAMÓWIENIA I MOŻLIWOŚCI SKŁADANIA OFERT CZĘŚCIOWYCH

Dotyczy części 1, 2, 3,

1. Zamawiający dopuszcza składanie ofert częściowych.
2. Zamówienie zostało podzielone na 4 części:

Część 1: Stacje robocze – 15 sztuk wraz z monitorami i oprogramowaniem, Tablety – 18 sztuk

Część 2: serwer – 1 sztuka

Część 3: Zakup i konfiguracja oprogramowania firewall

3.Szczegółowy zakres prac zawarty został w SWZ – opis przedmiotu zamówienia

4. Wykonawca może złożyć ofertę na jedną lub więcej części

## ROZDZIAŁ XVIII. INFORMACJA DOTYCZĄCA MOŻLIWOŚCI SKŁADANIA OFERT

### WARIANTOWYCH

Dotyczy części 1, 2, 3,

Zamawiający nie przewiduje możliwości składania ofert wariantowych.

### ROZDZIAŁ XIX. SPOSÓB OBLICZENIA CENY

Dotyczy części 1, 2, 3,

1. Oferta powinna być sporządzona na formularzu ofertowym, w języku polskim, w formie elektronicznej, podpisana podpisem kwalifikowanym, lub w postaci elektronicznej podpisanej profilem zaufanym lub osobistym przez osobę upoważnioną – załącznik nr 1
2. W ofercie należy podać cenę zamówienia, przez którą należy rozumieć cenę w rozumieniu art. 3 ust.1 pkt 1 i ust. 2 ustawy z dnia 9 maja 2014 r. o informowaniu o cenach towarów i usług (Dz.U. z 2019 poz.178).
3. Podana w ofercie cena musi być wyrażona w PLN.
4. Wykonawca zobowiązany jest podać cenę netto i brutto za realizację całości przedmiotu zamówienia określonego w rozdziale III SWZ, z wyszczególnionym podatkiem VAT.
5. Zastosowane materiały mają posiadać odpowiednie certyfikaty, aprobaty techniczne lub deklaracje zgodności dopuszczające do stosowania w budownictwie i atesty.
6. Cena musi uwzględniać wszystkie wymagania niniejszej SWZ oraz obejmować wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia.
7. Jeżeli złożono ofertę, której wybór prowadziłby do powstania obowiązku podatkowego Zamawiającego zgodnie z przepisami o podatku od towarów i usług w zakresie dotyczącym wewnątrzwspólnotowego nabycia towarów, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek wpłacić zgodnie zobowiązującymi przepisami. W ofercie, o której wykonawca ma obowiązek:
   1. poinformowania zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego;
   2. wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
   3. wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;
   4. wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.
8. Sposób zapłaty i rozliczenia za realizację niniejszego zamówienia, określone zostały we wzorze umowy stanowiącym załącznik do niniejszej SWZ.
9. Zamawiający poprawi w ofercie oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek, stosownie do treści art. 223 ust. 2 Pzp. Zamawiający zawiadomi Wykonawcę, którego oferta została poprawiona.
10. W przypadku podejrzeń zaoferowania w ofercie rażąco niskiej ceny Zamawiający przeprowadzi procedurę wyjaśniającą zgodnie z art. 224 ustawy Pzp.
11. Cena za wykonanie przedmiotu zamówienia podana przez Wykonawcę w formularzu ofertowym, wyliczona na podstawie kosztorysu ofertowego jest stałą ceną ryczałtową. Powyższe nie odnosi się do realizacji dodatkowych dostaw, usług lub robót budowlanych oraz robót zamiennych – w tym zakresie wynagrodzenie ma charakter kosztorysowy. Szczegółowe postanowienia dotyczące zakresu robót do których odnosi się wynagrodzenie ryczałtowe lub kosztorysowe oraz sposobu rozliczania zawierają projektowane postanowienia umowy, które zostaną wprowadzone do treści tej umowy, stanowiące załącznik do SWZ.

### ROZDZIAŁ XX. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

Dotyczy części 1, 2, 3,

1. Zamawiający oceni i porówna jedynie te oferty, które:

1) zostaną złożone przez Wykonawców niewykluczonych przez Zamawiającego 2) nie zostaną odrzucone przez Zamawiającego.

1. Przy wyborze oferty najkorzystniejszej, Zamawiający będzie się kierował następującymi kryteriami:

|  |  |  |  |
| --- | --- | --- | --- |
| L.P. | Nazwa kryterium | Waga % | Maksymalna liczba punktów |
| 1. | Cena ofertowa brutto | 60 | 60 |
| 2. | Gwarancja | 40 | 40 |

* 1. CENA BRUTTO – WAGA 60% maksymalna ilość punktów do zdobycia – 60

Kryterium będzie oceniane na podstawie ceny brutto podanej w formularzu ofertowym wg poniższego wzoru:

najniższa oferowana cena spośród wszystkich ważnych nieodrzuconych ofert

Liczba pkt = …………………………………….….……………………..…….……………………… x 60 cena badanej oferty

* 1. KRYTERIUM GWARANCJA

Za każdy 1 rok udzielonej gwarancji powyżej wymaganych min. 2 lat . Wykonawca otrzyma punkty zgodnie z poniższym maksymalnie 40 pkt, za 4 i więcej lat okresu gwarancji.

Gwarancja 2 lata - 0 punktów – wymagana długość gwarancji

Gwarancja 3 lata – 20 punktów

Gwarancja 4 lat i więcej – 40 punktów

UWAGA Wykonawca w formularzu oferty jest zobligowany określić gwarancję min. 2 lata, każde kolejne lata będę punktowane zgodnie z powyższą zasadą. Inne wartości będą zaniżane w dół (np. liczba 2 i 9 miesięcy będzie traktowana jako 2 lata). W przypadku wpisania w formularzu oferty gwarancji niższej niż 2 lata oferta zostanie odrzucona jako niezgodna z SWZ.

1. Wybrana zostanie oferta, która uzyska najwyższą łączną ilość punktów w powyższych kryteriach. Maksymalna łączna ilość punktów do zdobycia – 100.
2. Zamawiający poprawi w ofercie oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe, inne omyłki polegające na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, niepowodujące istotnych zmian w treści oferty.
3. Każdy z Wykonawców otrzyma odpowiednią ilość punktów, wyliczoną o powyższe kryteria. Będzie ona stanowiła składową uzyskanych punktów w każdym kryterium. Wykonawca może uzyskać max. 100 pkt.
4. Przy obliczaniu punktów Zamawiający zastosuje zaokrąglenia 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 ulegnie zmianie.

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

### ROZDZIAŁ XXI. WYMAGANIA DOTYCZĄCE WADIUM

Dotyczy części 1, 2, 3,

Zamawiający nie wymaga wniesienia wadium.

### ROZDZIAŁ XXII. INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 214 UST. 1 PKT. 7 I 8

Dotyczy części 1, 2, 3,

Zamawiający nie przewiduje udzielania takich zamówień.

### ROZDZIAŁ XXIII. INFORMACJE DOTYCZĄCE WIZJI LOKALNEJ

Dotyczy części 1, 2, 3,

Zamawiający nie przewiduje obowiązku przeprowadzenia wizji lokalnej.

### ROZDZIAŁ XXIV. INFORMACJE DOTYCZACE ZWROTU KOSZTÓW UDZIALU W POSTĘPOWANIU

Dotyczy części 1, 2, 3,

Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

### ROZDZIAŁ XXV. INFORMACJA DOTYCZĄCA UMOWY RAMOWEJ

Dotyczy części 1, 2, 3,

Zamawiający nie przewiduje zawarcia umowy ramowej.

### ROZDZIAŁ XXVI. INFORMACJA DOTYCZACA AUKCJI ELEKTRONICZNEJ

Dotyczy części 1, 2, 3,

Zamawiający nie przewiduje aukcji elektronicznej.

### ROZDZIAŁ XXVII. INFORMACJA DOTYCZĄCA ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Dotyczy części 1, 2, 3,

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

### ROZDZIAŁ XXVIII. INFORMACJA O ŚRODKACH OCHRONY PRAWNEJ

Dotyczy części 1, 2, 3,

1. Zasady, terminy oraz sposób korzystania ze środków ochrony prawnej szczegółowo regulują przepisy działu IX ustawy – Środki ochrony prawnej (art. 513 – 521 ustawy).
2. Środki ochrony prawnej określone w dziale VI przysługują Wykonawcy, uczestnikowi konkursu, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy.
3. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz SWZ, przysługują również organizacjom wpisanym na listę organizacji uprawnionych do wnoszenia środków ochrony prawnej, prowadzoną przez Prezesa Urzędu Zamówień Publicznych.
4. Terminy wnoszenia odwołań:
   1. Odwołanie wnosi się przy zamówieniach których wartość jest równa lub przekracza progi unijne:
      1. w terminie 10 dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia przy użyciu środków komunikacji elektronicznej
      2. w terminie 15 dni – jeżeli informacja została przekazana w inny sposób, 2) Dla zamówień poniżej progów unijnych:
      3. w terminie 5 dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia przy użyciu środków komunikacji elektronicznej
      4. w terminie 10 dni – jeżeli informacja została przekazana w inny sposób
   2. Odwołanie wobec treści ogłoszenia o zamówieniu oraz wobec postanowień SWZ, wnosi się w terminie: 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia SWZ na stronie internetowej, oraz 5 dni od dnia publikacji ogłoszenia w BZP lub dokumentów zamówienia na stronie Zamawiającego – dla zamówień poniżej progów unijnych.
   3. Odwołanie wobec czynności innych niż określone w pkt. 4.1. i 4.2. wnosi się:
   4. w terminie 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia – dla zamówień o wartości równej lub wyższej niż progi unijne, oraz 5 dni – dla zamówień poniżej progów unijnych.
5. Odwołanie przysługuje wyłącznie od niezgodnej przepisami ustawy czynności Zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której Zamawiający jest zobowiązany na podstawie ustawy.
   1. Odwołanie powinno wskazywać czynności lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami ustawy, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.
   2. Odwołanie wnosi się do Prezesa Izby w formie pisemnej w postaci papierowej albo postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.
   3. Odwołanie podlega rozpoznaniu, jeżeli:
      1. nie zawiera braków formalnych;
      2. uiszczono wpis (wpis uiszcza się najpóźniej do dnia upływu terminu do wniesienia odwołania, a dowód jego uiszczenia dołącza się do odwołania).
   4. Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, iż Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
6. Na orzeczenie Izby stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
   1. W postępowaniu toczącym się wskutek wniesienia skargi stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego o apelacji, jeżeli przepisy ustawy nie stanowią inaczej. Jeżeli koniec terminu do wykonania czynności przypada na sobotę lub dzień ustawowo wolny od pracy, termin upływa dnia następnego po dniu lub dniach wolnych od pracy.
   2. Skargę wnosi się do sądu właściwego dla siedziby albo miejsca zamieszkania zamawiającego za pośrednictwem Prezesa Izby w terminie 7 dni od dnia doręczenia orzeczenia Izby, przesyłające jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego jest równoznaczne z jej wniesieniem.
   3. W terminie 21 dni od dnia wydania orzeczenia skargę może wnieść także Prezes Urzędu. Prezes Urzędu może także przystąpić do toczącego się postępowania. Do czynności podejmowanych przez Prezesa Urzędu stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego o prokuraturze.
   4. Skarga powinna czynić zadość wymaganiom przewidzianym dla pisma procesowego oraz zawierać oznaczenie zaskarżonego orzeczenia, przytoczenie zarzutów, zwięzłe ich uzasadnienie, wskazanie dowodów, a także wniosek o uchylenie orzeczenia lub zmianę orzeczenia w całości lub w części.
   5. W postępowaniu toczącym się na skutek wniesienia skargi nie można rozszerzyć żądania odwołania ani występować z nowymi żądaniami.

### ROZDZIAŁ XXIX. OPIS SPOSOBU UDZIELANIA WYJASNIEŃ DOTYCZĄCYCH SPECYFIKACJI WARUNKÓW ZAMÓWIENIA

Dotyczy części 1, 2, 3,

1. Na podstawie art. 284 ustawy Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SWZ.
2. Zamawiający niezwłocznie udzieli wyjaśnień, jednakże nie później niż na 2 dni przed upływem terminu składania ofert, o ile wniosek o wyjaśnienie Specyfikacji wpłynie do Zamawiającego nie później niż na 4 dni przed upływem wyznaczonego terminu składania ofert.
3. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ. Każda wprowadzona przez Zamawiającego zmiana staje się w takim przypadku częścią Specyfikacji. Dokonaną zmianę treści SWZ Zamawiający udostępnia na stronie internetowej pod adresem: www.bip.starozreby.pl
4. Zamawiający oświadcza, iż nie zamierza zwoływać zebrania Wykonawców w celu wyjaśnienia treści SWZ.
5. Treść niniejszej SWZ zamieszczona jest na stronie internetowej, pod następującym adresem:

www.bip.starozreby.pl Wszelkie zmiany treści SWZ, jak też wyjaśnienia i odpowiedzi na pytania co do treści SWZ, Zamawiający zamieszczać będzie także pod wskazanym wyżej adresem internetowym.

### ROZDZIAŁ XXX. INFORMACJA NA TEMAT ROZLICZANIA SIĘ W WALUTACH OBCYCH

Dotyczy części 1, 2, 3,

Zamawiający będzie rozliczał się z Wykonawcą wyłącznie z uwzględnieniem waluty polskiej.

### ROZDZIAŁ XXXI. INFORMACJA O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

Dotyczy części 1, 2, 3,

1. Zamawiający zawiadomi niezwłocznie Wykonawców, którzy ubiegali się o udzielenie zamówienia o:

1. wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania, jeżeli jest miejscem wykonywania działalności wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania, jeżeli są miejscami wykonywania działalności wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację,
2. wykonawcach, których oferty zostały odrzucone - podając uzasadnienie faktyczne i prawne.
3. Zamawiający zawrze umowę w sprawie zamówienia publicznego w terminie określonym w art. 264 ust. ustawy Pzp w siedzibie Zamawiającego lub w formie elektronicznej.
4. Zamawiający powiadomi drogą elektroniczną Wykonawcę, którego oferta została wybrana o terminie zawarcia umowy.
5. Jeżeli Wykonawca, którego oferta została wybrana, będzie się uchylał od zawarcia umowy w sprawie zamówienia publicznego, Zamawiający wybierze ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownej oceny.

### ROZDZIAŁ XXXII. INFORMACJE DOTYCZĄCE UMOWY

Dotyczy części 1, 2, 3,

1. Istotne dla Zamawiającego postanowienia umowy, zawiera załączony do niniejszej SWZ wzór umowy.

1) Zamawiający przewiduje możliwość zmian postanowień zawartej umowy,

w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy zgodnie z warunkami podanymi we wzorze umowy, stanowiącym załącznik do SWZ.

1. Zmiana umowy może także nastąpić w przypadkach, o których mowa w art. 454 i 455 ustawy PZP. Zmiany umowy zostały określone w projekcie umowy.
2. Umowa w sprawie zamówienia publicznego może zostać zawarta wyłącznie z Wykonawcą, którego oferta zostanie wybrana jako najkorzystniejsza, po upływie terminów określonych w art. 264 ustawy.
3. W przypadku wniesienia odwołania, aż do jego rozstrzygnięcia, Zamawiający wstrzyma podpisanie umowy.

4. W przedmiotowym postępowaniu zostanie zawarta umowa pomiędzy Wójtem Gminy Staroźreby reprezentującym Gminę Staroźreby a Wykonawcą.

### ROZDZIAŁ XXXIII. RODO

Dotyczy części 1, 2, 3,

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

1. administratorem Pani/Pana danych osobowych jest Wójt Gminy Staroźreby, Urząd Gminy w Staroźrebach przy ul. Płockiej 18, 09-440 Staroźreby
2. inspektorem ochrony danych osobowych w Gminie Staroźreby jest Inspektor ds. danych osobowych, z którym skontaktować się można – mail: iod@starozreby.pl tel. 24 266 30 86. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. C RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego Dostawa sprzętu komputerowego dla gminy Staroźreby w ramach projektu grantowego Cyfrowa Gmina prowadzonym w trybie podstawowym;
3. przetwarzane będą na podstawie art. 6 ust. 1 lit. C RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego /dane identyfikujące postępowanie, np. nazwa, numer/ prowadzonym w trybie podstawowym;
4. odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 78 ustawy Prawo zamówień publicznych, dalej „ustawa Pzp”;
5. obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
6. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO; 7) posiada Pani/Pan:

− na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;

− na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych \*\*;

− na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;

− prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO; 8) nie przysługuje Pani/Panu:

− w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

− prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

− na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

Wykaz załączników do SWZ.

1. Załącznik nr 1 – formularz ofertowy
2. Załącznik nr 2 – oświadczenie Wykonawcy art.125 ust.1 Pzp
3. Załącznik nr 3 - Projekt umowy
4. Załącznik nr 4 –oświadczenie w zakresie art. 108 ust.1 pkt 5 ustawy Pzp
5. Załącznik nr 5 – oświadczenie wykonawców wspólnie ubiegających się o udzielenie zamówienia
6. Załącznik nr 6 – Wykaz dostaw
7. Załącznik nr 7 - zobowiązanie podmiotu trzeciego.