Znak sprawy: ZP.271.17.2025

ZAMAWIAJĄCY
GMINA ŻUKOWO

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA (SWZ)

na

„Dostawę urządzeń UTM i przełączników sieciowych”

Postępowanie prowadzone na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz.U. z 2024 r. poz. 1320), zwana dalej Pzp, przepisów wykonawczych wydanych na jej podstawie oraz niniejszej Specyfikacji Warunków Zamówienia (SWZ).

Zatwierdziła:

z up. Burmistrza
Karolina Redzimska
Zastępca Burmistrza

Znak sprawy: ZP.271.17.2025

SPIS TREŚCI

Znak sprawy: ZP.271.17.2025

I. Nazwa, adres i inne dane zamawiającego

GMINA ŻUKOWO, ul. Gdańska 52, 83-330 Żukowo

NIP 589-001-16-54, REGON 191675095

tel. +48 58 6858318, fax +48 58 6858330

Adres strony internetowej: www.zukowo.pl

Adres poczty elektronicznej: ugzukowo@zukowo.pl

Adres platformy do obsługi niniejszego postępowania (adres strony internetowej, na której jest prowadzone postępowanie i na której będą dostępne wszelkie dokumenty związane z prowadzonym postępowaniem):

https://platformazakupowa.pl/transakcja/1100460

II. Ochrona danych osobowych

Ochrona danych osobowych zebranych przez Zamawiającego w toku postępowania – klauzula informacyjna z art. 13 i 14 RODO.

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 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 4.5.2016 r., str. 1), dalej „RODO", Zamawiający informuje, że:

1. W okresie obejmującym wszczęcie i przeprowadzenie postępowania o udzielenie zamówienia publicznego oraz z chwilą zawarcia umowy Administratorem danych osobowych jest Gmina Żukowo, której dane kontaktowe są następujące:

- adres korespondencyjny: ul. Gdańska 52, 83-330 Żukowo
- adres e-mail: ugzukowo@zukowo.pl.

2. We wszystkich sprawach dotyczących ochrony danych osobowych w okresie obejmującym wszczęcie i przeprowadzenie postępowania o udzielenie zamówienia publicznego, ma Pani/Pan prawo kontaktować się z Inspektorem Ochrony Danych na adres e-mail: iod@zukowo.pl.

3. Pani/Pana dane osobowe przetwarzane będą w celu przeprowadzenia przedmiotowego postępowania o udzielenie zamówienia publicznego prowadzonego na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych oraz jego rozstrzygnięcia, jak również zawarcia umowy w sprawie zamówienia publicznego oraz jej realizacji, a także udokumentowania postępowania o udzielenie zamówienia publicznego i jego archiwizacji.

4. Jeżeli Wykonawca prowadzi jednoosobową działalność gospodarczą lub jest wspólnikiem spółki cywilnej to podstawą przetwarzania jest art. 6 ust. 1 lit. b) RODO w celu zawarcia i wykonania umowy.
5. Podstawą przetwarzania danych osobowych jest art. 6 ust. 1 lit. c) RODO – przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze w związku z:
   1) ustawą z dnia 11 września 2019 r. - Prawo zamówień publicznych (t.j. Dz.U. 2023 poz. 1605 ze zm.);
   2) ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz.U. 2020 poz. 164 ze zm).
6. Podstawą przetwarzania danych osób reprezentujących strony umów, wyznaczonych do kontaktów roboczych/służbowych podczas przeprowadzenia przedmiotowego postępowania lub osób odpowiedzialnych za koordynację i realizację umowy jest prawnie uzasadniony interes Zamawiającego (art. 6 ust. 1 lit. f) RODO), polegający na umożliwieniu kontaktu pomiędzy stronami umów lub jej sprawną realizacją.
7. Odbiorcami danych osobowych są podmioty upoważnione na podstawie zawartych umów powierzenia, w tym Open Nexus Sp. z o.o. jako właściciela Platformy zakupowej, oraz uprawnione na mocy obowiązujących przepisów prawa, w szczególności osoby lub podmioty, którym zostanie udostępniona dokumentacja postępowania na podstawie art. 18 oraz art. 74 ustawy Pzp. Zasada jawności ma zastosowanie do wszystkich danych osobowych, z wyjątkiem danych, o których mowa w art. 9 ust. 1 RODO (szczególna kategoria danych).
8. Jeśli przedmiotem zamówienia są: Fundusze Europejskie dla Pomorza 2021 - odbiorcą danych będzie Instytucja Zarządzająca Projektami Europejskimi.
9. Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do zrealizowania celu, po tym czasie dane osobowe będą przechowywane przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa.

Zamawiający będzie przechowywał protokół postępowania wraz z załącznikami przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, w sposób gwarantujący jego nienaruszalność.
Jeżeli okres obowiązywania umowy w sprawie zamówienia publicznego przekroczy 4 lata, Zamawiający przechowuje protokół postępowania wraz z załącznikami przez cały okres obowiązywania umowy w sprawie zamówienia publicznego.
Dane osobowe będą przechowywane do 31.12.2034 r. z uwzględnieniem czasu niezbędnego do osiągnięcia celu, w jakim je pozyskano, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa (jeśli przedmiotem zamówienia są Fundusze Europejskie: art. 82 Rozporządzenia

Parlamentu Europejskiego i Rady (UE) nr 2021/1060 z dnia 24 czerwca 2021 r.), tj. przez 10 lat od roku następnego po zakończeniu umowy.
Ponadto okres przechowywania musi być zgodny z terminami archiwizacji określonymi przez przepisy powszechnie obowiązującego prawa, w tym Rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

10. Posiada Pan/Pani:

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

    2) na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia Pani/Pana danych osobowych, przy czym skorzystanie z prawa do sprostowania lub uzupełnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu postępowania oraz jego załączników;

    3) 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, przy czym prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego, a także nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia;

    4) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-913 Warszawa), gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

11. Nie przysługuje Pani/Panu:

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

    2) 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.

12. Podanie danych osobowych jest wymogiem ustawowym określonym w ustawie Pzp, związanych z udziałem w postępowaniu o udzielenie zamówienia; konsekwencje niepodania określonych danych wynikają z ustawy Pzp.

13. W celu realizacji swoich prawa wynikających z RODO, należy skontaktować się z Inspektorem ochrony danych lub Administratorem na adres siedziby.
14. Źródłem danych osobowych jest Wykonawca.
15. Kategorie danych osobowych: dane teleadresowe (m.in.: adres korespondencyjny, adres e-mail, nr telefonu) oraz identyfikacyjne (m.in.: imię i nazwisko).
16. Jednocześnie Zamawiający zobowiązuje Wykonawcę do przekazania powyższych informacji, w celu spełnienia obowiązku informacyjnego ciążącego na Administratorze na podstawie art. 14 RODO, względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od Wykonawcy biorącego udział w postępowaniu.

III. Tryb udzielania zamówienia

1. Postępowanie prowadzone jest w trybie podstawowym, na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych. Zamawiający nie przewiduje prowadzenia negocjacji.
2. Szacunkowa wartość przedmiotowego zamówienia nie przekracza progów unijnych, o jakich mowa w art. 3 ustawy PZP (tj. progu unijnego).
3. Zamawiający nie przewiduje aukcji elektronicznej.
4. Zamawiający nie prowadzi postępowania w celu zawarcia umowy ramowej.
5. Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez Wykonawców, o których mowa w art. 94 PZP
6. Wymagania związane z realizacją zamówienia w zakresie zatrudnienia na podstawie stosunku pracy, w okolicznościach, o których mowa w art. 96 Pzp. Zamawiający nie stawia takich wymagań.
7. Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 8 ustawy PZP.
8. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SWZ nie później niż na 4 dni przed upływem terminu składania ofert. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert. Przedłużenie terminu składania ofert nie wpływa na bieg terminu

składania wniosku o wyjaśnienie treści SWZ. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ. Treść zapytań wraz z wyjaśnieniami oraz dokonaną zmianę SWZ Zamawiający udostępnia na stronie internetowej prowadzonego postępowania w zakładce dedykowanej postępowaniu.

9. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu z zastrzeżeniem art. 261 ustawy PZP.

IV. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest dostawa dwóch urządzeń UTM i dwudziestu przełączników sieciowych" dla Urzędu Gminy w Żukowie i Gminnego Ośrodka Pomocy Społecznej w Żukowie w ramach projektu „Cyberbezpieczny Samorząd.

1.2. Szczegółowy opis przedmiotu zamówienia:

SYSTEM BEZPIECZEŃSTWA – 1 szt. Urządzenie UTM (Unified Threat Management) dla Urzędu Gminy w Żukowie	
Parametr	**Charakterystyka (wymagania minimalne)**
Wymagania ogólne	System bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. System powinien wspierać protokoły IPv4 oraz IPv6 w zakresie: 1. Firewall. 2. Ochrony w warstwie aplikacji. 3. 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 system firewall musi zapewniać funkcję synchronizacji sesji.

	2. System powinien posiadać funkcję monitoringu i wykrywanie uszkodzeń elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. System powinien posiadać funkcję monitoringu stanu realizowanych połączeń VPN. 4. System powinien umożliwiać agregację linków statycznych oraz w oparciu o protokół LACP oraz dawać możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall powinien dysponować co najmniej poniższą liczbą i rodzajem interfejsów: 1) 10 portami Gigabit Ethernet RJ-45. 2) 8 gniazdami SFP 1 Gbps. 3) 4 gniazdami SFP+ 10 Gbps. 2. System Firewall powinien posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 3. System Firewall powinien pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System realizujący funkcję Firewall powinien być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB. 5. System powinien być wyposażony w redundantne zasilanie (2xAC).
Parametry wydajnościowe	1. W zakresie Firewall'a powinien obsługiwać nie mniej niż 3 mln jednoczesnych połączeń oraz 260 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 26 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12.6 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 12 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) - minimum 4.8 Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3.9 Gbps.
Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony powinny 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. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

	10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 13. Rozwiązanie powinno posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	1. Polityka Firewall powinna uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System powinien realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 1) Translację jeden do jeden oraz jeden do wielu. 2) Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu powinien istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. System powinien dawać możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 5. Polityka firewall powinna umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. System powinien dawać możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall powinien 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. 1) Microsoft Azure. 2) Google Cloud Platform (GCP). 3) VMware NSX.
Połączenia VPN	1. System powinien umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji powinien zapewniać: 1) Wsparcie dla IKE v1 oraz v2. 2) Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). 3) Obsługa protokołu Diffie-Hellman grup 19, 20. 4) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. 5) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 6) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 7) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 8) Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. 9) Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

	10) Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. 11) Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. 12) Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System powinien umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewniać pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. 3. Producent rozwiązania musi posiadać w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest powinno być dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	System powinien pozwalać na zdefiniowanie: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu
Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN powinien wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall powinien umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP (Differentiated Services Code Point) oraz wskazanie priorytetu ruchu. 2. System powinien dawać możliwość określania pasma dla poszczególnych aplikacji. 3. System powinien pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System powinien zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy powinien zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych powinna istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwiać konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System powinien umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.

	5. System powinien dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System powinien współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. System powinien zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. System powinien mieć możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. System powinien mieć możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
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 powinien być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu powinien mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System powinien zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. System powinien posiadać mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. System powinien posiadać możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookiesdla protokołu http. 8. System powinien posiadać możliwość wykrywania i blokowania komunikacji C&C do sieci botnet. 9. System powinien posiadać możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
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 sygnatur powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu powinien mieć możliwość definiowania wyjątków oraz własnych sygnatur. 6. System powinien posiadać możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System powinien posiadać możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych

	protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	1. Moduł kontroli WWW powinien 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 powinien dostarczać kategorie stron zabronionych prawem np.: Hazard. 4. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW powinien umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW powinien umożliwiać wykonanie akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. System powinien posiadać funkcję Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator powinien mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System powinien pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall powinien umożliwiać weryfikację tożsamości użytkowników za pomocą: 1) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 2) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 3) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System powinien dawać możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. System powinien umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. System powinien posiadać możliwość uwierzytelniania 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 móc współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania powinna być realizowana z wykorzystaniem szyfrowanych protokołów. 3. W systemie powinna istnieć możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.

	4. System powinien móc współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System powinien dawać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall powinien posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall powinien umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. System powinien posiadać możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. System powinien posiadać możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa powinny realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne będzie zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall powinien zapewniać przekazywanie danych o: 1) zaakceptowanym ruchu, 2) blokowanym ruchu, 3) aktywności administratorów, 4) zużyciu zasobów oraz stanie pracy systemu. Ponadto powinien zapewniać możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie powinno obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. System powinien mieć możliwość włączenia logowania per reguła w polityce firewall. 5. System powinien zapewniać możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów powinno być możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

SYSTEM BEZPIECZEŃSTWA – 1 szt. Urządzenie UTM (Unified Threat Management) dla Gminnego Ośrodka Pomocy Społecznej w Żukowie	
Parametr	**Charakterystyka (wymagania minimalne)**
Wymagania ogólne	System bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być

	zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. System powinien wspierać protokoły IPv4 oraz IPv6 w zakresie: 1. Firewall. 2. Ochrony w warstwie aplikacji. 3. 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 system firewall musi zapewniać funkcję synchronizacji sesji. 2. System powinien posiadać funkcję monitoringu i wykrywanie uszkodzeń elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. System powinien posiadać funkcję monitoringu stanu realizowanych połączeń VPN. 4. System powinien umożliwiać agregację linków statycznych oraz w oparciu o protokół LACP oraz dawać możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall powinien dysponować co najmniej 5 portami Gigabit Ethernet RJ-45. 2. System Firewall powinien posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 3. System Firewall powinien pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System powinien być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a powinien obsługiwać nie mniej, niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) - minimum 1 Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony powinny 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. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 13. Rozwiązanie powinno posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	1. Polityka Firewall powinna uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System powinien realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 1) Translację jeden do jeden oraz jeden do wielu. 2) Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu powinien istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. System powinien dawać możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 5. Polityka firewall powinna umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. System powinien dawać możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall powinien 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. 1) Microsoft Azure. 2) Google Cloud Platform (GCP). 4) VMware NSX
Połączenia VPN	1. System powinien umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: 1) Wsparcie dla IKE v1 oraz v2.

	2) Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). 3) Obsługa protokołu Diffie-Hellman grup 19, 20. 4) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. 5) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 6) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 7) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 8) Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. 9) Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. 10) Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. 11) Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. 12) Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. Producent rozwiązania powinien posiadać w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	System powinien pozwalać na zdefiniowanie: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu
Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN powinien wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall powinien umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP (Differentiated Services Code Point) oraz wskazanie priorytetu ruchu. 2. System powinien dawać możliwość określania pasma dla poszczególnych aplikacji. 3. System powinien pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System powinien zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

	2. Silnik antywirusowy powinien zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych powinna istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwiać konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System powinien umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System powinien dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System powinien współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. System powinien mieć możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 9. System powinien mieć możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
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 powinien być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu powinien mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System powinien zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. System powinien posiadać mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. System powinien posiadać możliwość wykrywania i blokowania komunikacji C&C do sieci botnet. 8. System powinien posiadać możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
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 sygnatur powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

	5. Administrator systemu powinien mieć możliwość definiowania wyjątków oraz własnych sygnatur. 6. System powinien posiadać możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System powinien posiadać możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	1. Moduł kontroli WWW powinien 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 powinien dostarczać kategorie stron zabronionych prawem np.: Hazard. 4. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW powinien umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW powinien umożliwiać wykonanie akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. System powinien posiadać funkcję Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator powinien mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System powinien pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall powinien umożliwiać weryfikację tożsamości użytkowników za pomocą: 1) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 2) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 3) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System powinien dawać możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. System powinien umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. System powinien posiadać możliwość uwierzytelniania 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 móc współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.

	2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania powinna być realizowana z wykorzystaniem szyfrowanych protokołów. 3. W systemie powinna istnieć możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System powinien móc współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System powinien dawać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall powinien posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall powinien umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. System powinien posiadać możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. System powinien posiadać możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa powinny realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne będzie zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall powinien zapewniać przekazywanie danych o: 1) zaakceptowanym ruchu, 2) blokowanym ruchu, 3) aktywności administratorów, 4) zużyciu zasobów oraz stanie pracy systemu. zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie powinno obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. System powinien mieć możliwość włączenia logowania per reguła w polityce firewall. 5. System powinien zapewniać możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów powinno być możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

Przełączniki sieciowe - 20 szt.	
Parametr	**Charakterystyka (wymagania minimalne)**

Wymagania ogólne	W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełączników oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa posiadających rozwiązanie, które umożliwi zarządzanie przełącznikami z poziomu oferowanego systemu bezpieczeństwa lub systemu opartego na rozwiązaniach chmurowych, jednak takie rozwiązanie musi posiadać możliwość zarządzania wspólnego i jednolitego dla systemów bezpieczeństwa oraz przełączników sieciowych.
Parametry fizyczne platformy	1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. 2. Wymagane zasilanie AC 230V. 3. Maksymalny pobór mocy: 30 W. 4. Minimalny zakres temperatury pracy: 0-40^{o}C.
Interfejsy sieciowe - wymagania minimalne	Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: 1. 24 porty GE RJ-45. 2. 4 porty 10 GE SFP+.
Zarządzanie	1. Minimum jeden wbudowany port konsoli szeregowej do pełnego zarządzania. 2. Urządzenie musi umożliwiać zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki z obsługą HTTPS. 3. Urządzenie powinno mieć wsparcie dla SNMP w wersjach 1-3 4. Urządzenie powinno być wyposażony w funkcję zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. 5. Urządzenie powinno posiadać funkcję aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. 6. Urządzenie powinno posiadać możliwość konfiguracji w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. 7. Urządzenie powinno posiadać funkcję backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). 8. Urządzenie powinno posiadać funkcję definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. 9. Urządzenie powinno posiadać funkcję definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. 10. Urządzenie powinno posiadać funkcję automatycznego wykonywania rewizji konfiguracji
Parametry wydajnościowe	1. Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach). 2. Tablica adresów MAC o pojemności co najmniej 32k wpisów. 3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
Wymagane funkcje	1. Urządzenie powinno posiadać funkcję automatycznej negocjacji prędkości i duplexu dla połączeń. 2. Urządzenie powinno posiadać obsługę Jumbo Frames.

	3. Urządzenie powinno posiadać obsługę protokołów 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). 4. Urządzenie powinno móc agregować porty zgodne ze standardem 802.3ad. 1. Urządzenie powinno posiadać obsługę co najmniej 500 VLAN'ów, zgodna ze standardem 802.1Q. 2. Urządzenie powinno posiadać obsługę routingu statycznego. 3. Urządzenie powinno posiadać funkcję Port-mirroring. 4. Urządzenie powinno być wyposażone w mechanizmy uwierzytelniania 802.1x na poziomie portu. 5. Urządzenie powinno być wyposażone w mechanizmy uwierzytelniania 802.1x w oparciu o adres MAC. 6. W ramach 802.1x powinno popsiadać wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). 7. W ramach 802.1x powinno posiadać wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. 8. W ramach 802.1x powinno posiadać wsparcie dla dynamicznego przypisywania VLAN. 9. Urządzenie powinno posiadać obsługę protokołu sFlow.
Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania	1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: 1) centralne zarządzanie konfiguracją urządzenia 2) aktualizację oprogramowania realizowaną z systemu centralnego zarządzania 3) centralne zarządzanie sieciami VLAN. 4) blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u 5) rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. 6) przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. 7) integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. 8) automatyczną detekcję i rekomendacje konfiguracji. 9) przesyłanie logów na zewnętrzny serwer syslog. 10) funkcję uruchomienia Captive Portalu w celu identyfikacji użytkowników. 11) obsługę białych i czarnych list adresów MAC. 12) wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. 2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Wymagania wspólne dla oferowanych produktów	
Parametr	**Charakterystyka (wymagania minimalne)**
Wymagania ogólne	1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. 3. Opakowania oferowanych produktów muszą być wykonane z materiałów podlegających powtórnemu przetworzeniu, 4. Zamawiający wymaga dokumentację w języku polskim lub angielskim. 5. Wykonawca zobowiązany będzie przedłożyć dokument świadczący, że oferowany przedmiot zamówienia posiada deklarację zgodności CE. 6. Wykonawca zobowiązany będzie przedłożyć dokument, który jest potwierdzeniem, że oferowany przedmiot zamówienia spełnia wymagania dyrektywy ROHS 2011/65/UE z dnia 8 czerwca 2011 r. na temat zakazu użycia niebezpiecznych substancji w wyposażeniu elektrycznym i elektronicznym (RoHS - restriction of the use of certain hazardous substances) lub spełniać warunki równoważności w postaci przedstawienia CERTYFIKATU wystawionego przez niezależną, akredytowaną jednostkę, potwierdzającego zgodność urządzeń komputerowych z dyrektywą RoHS – (ang. Restriction of Hazardous Substances), z 27 stycznia 2003 r. (2002/95/EC), wprowadzoną w życie 1 lipca 2006 r., dyrektywa ta została transponowana do Rzeczypospolitej Polskiej rozporządzeniem Ministra Gospodarki z dnia 27 marca 2007 r. w sprawie szczegółowych wymagań dotyczących ograniczenia wykorzystywania w sprzęcie elektronicznym i elektrycznym niektórych substancji mogących negatywnie oddziaływać na środowisko (Dz. U. poz. 457) – ostatnia aktualizacja - Dz. U. 2019 poz. 1277 - rozporządzenie Ministra Przedsiębiorczości i Technologii z dnia 24 czerwca 2019 r. zmieniające rozporządzenie w sprawie zasadniczych wymagań dotyczących ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym 7. Oferowane produkty muszą być fabrycznie nowe, nie używane, kompletne, sprawne technicznie, nie powystawowe oraz sprawnie technicznie.

Gwarancja oraz wsparcie	Oferowane produkty muszą być objęte serwisem gwarancyjnym producenta przez okres minimum12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (Advanced Hardware Replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7
Serwisy i licencje	1. System winien być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres objęty gwarancją. 2. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7

2. Urządzenia, o których mowa powyżej muszą być:
   a) fabrycznie nowe (nieregenerowane, nieużywane, nienaprawiane), pozbawione wad i uszkodzeń, kompletne (ze wszystkimi podzespołami, częściami, materiałami niezbędnymi do uruchomienia i użytkowania), sprawne technicznie, nie powystawowe i są gotowe do użycia;
   b) posiadać stosowne certyfikaty, w zakresie bezpieczeństwa odpowiadają normom CE oraz są dopuszczone do sprzedaży i użytkowania na terenie RP;
   c) zakup i korzystanie z urządzeń zgodnie z przeznaczeniem nie narusza prawa, w tym praw osób trzecich.

3. Zamawiający wymaga udzielenie przez Wykonawcę minimum 12 miesięcznej gwarancji dla wszystkich urządzeń będących przedmiotem zamówienia. Okres gwarancji stanowi jedno z kryteriów oceny ofert.

4. We wszystkich zapisach SWZ oraz jej załącznikach (w tym w projekcie umowy), w których Zamawiający, ze względu na brak możliwości opisania przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób, odwołuje się do norm, ocen technicznych, specyfikacji technicznych lub systemów referencji technicznych, bądź wskazane są znaki towarowe, patenty, źródła pochodzenia lub szczególne procesy, które charakteryzują produkty lub usługi dostarczane przez konkretnego wykonawcę, Zamawiający dopuszcza rozwiązania równoważne opisywanym.
   W przypadku, gdy w opisie przedmiotu zamówienia podano nazwy produktów konkretnych producentów to należy traktować to jedynie jako określenie pożądanego standardu i jakości. We wszystkich takich sytuacjach Wykonawca może zaoferować równoważne materiały, produkty o co najmniej takich samych parametrach technicznych oraz jakościowych. Przez równoważność produktu rozumie się zaoferowanie produktu, którego parametry techniczne

zastosowanych materiałów, wydajność, trwałość oraz jakość jest nie gorsza od jakości produktów opisanych w SWZ.

5. Wspólny Słownik Zamówień CPV:

   32413100-2 Rutery sieciowe
   32420000-3 Urządzenia sieciowe

6. Znak sprawy: ZP.271.17.2025
7. Wykonanie przedmiotu zamówienia musi być zgodne z niniejszą Specyfikacją Warunków Zamówienia (dalej: SWZ) oraz obowiązującymi przepisami prawa.
8. Zamawiający nie dopuszcza składanie ofert częściowych.
9. Zamawiający nie dopuszcza składania ofert wariantowych oraz w postaci katalogów elektronicznych.
10. Informacje dot. przeprowadzenia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2 ustawy PZP: Zamawiający nie stawia takich wymogów.
11. Zamówienie jest współfinansowane ze środków Unii Europejskiej w ramach Projektu grantowego „Cyberbezpieczny Samorząd”.

V. Podwykonawstwo

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom).
2. Informacja o obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań, jeżeli Zamawiający dokonuje takiego zastrzeżenia zgodnie z art. 60 i art. 121 ustawy PZP: Zamawiający nie wprowadza takiego zastrzeżenia. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy/ podwykonawcom. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
3. Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, Wykonawca wskazał w ofercie części zamówienia, których

wykonanie zamierza powierzyć podwykonawcom oraz podał (o ile są mu wiadome na tym etapie) nazwy (firmy) tych podwykonawców.

VI. Okres realizacji zamówienia

1. Termin wykonania zamówienia wynosi: 45 dni od dnia zawarcia umowy.
   Zamawiający dopuszcza wcześniejszą realizację przedmiotu zamówienia. W podanym terminie należy dokonać dostawy kompletnego przedmiotu zamówienia. Przed przystąpieniem do realizacji fizycznej dostawy tj. transportu sprzętu do Zamawiającego należy potwierdzić gotowość odbioru dostawy przez Zamawiającego.

VII. Warunki udziału w postępowaniu

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na zasadach określonych w Rozdziale VIII SWZ oraz spełniają określone przez Zamawiającego warunki udziału w postępowaniu dotyczące:
   1) zdolności do występowania w obrocie gospodarczym: Zamawiający nie precyzuje warunku w tym zakresie.
   2) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów Zamawiający nie precyzuje warunku w tym zakresie.
   3) sytuacji ekonomicznej lub finansowej: Zamawiający nie precyzuje warunku w tym zakresie.
   4) zdolności technicznej lub zawodowej. Zamawiający nie precyzuje warunku w tym zakresie.
2. Udostępnienie zasobów - poleganie na zdolnościach innych podmiotów.
   W związku z odstąpieniem zamawiającego od stawiania warunków udziału w postępowaniu nie mają zastosowania w niniejszym postępowaniu przepisy ustawy PZP dot. udostępniania zasobów.

3. Wspólne ubieganie się o udzielenie zamówienia.

1) Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo powinno być załączone do oferty.
2) dokument potwierdzający ustanowienie pełnomocnictwa powinien zawierać wskazanie:
   - postępowania o udzielenie zamówienia publicznego, którego dotyczy,
   - wykonawców ubiegających się wspólnie o udzielenie zamówienia,
   - ustanowionego pełnomocnika oraz zakres jego umocowania,

pełnomocnictwo musi być podpisane przez osoby upoważnione do składania oświadczeń woli w imieniu poszczególnych wykonawców.

3) w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia:
   - żaden z wykonawców wspólnie ubiegających się o udzielenie zamówienia nie może podlegać wykluczeniu w okolicznościach o których mowa w Rozdziale VIII SWZ,

4) oświadczenie i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z wykonawców wspólnie ubiegających się o zamówienie,
5) oświadczenie i dokumenty potwierdzające spełnianie warunków udziału w postępowaniu składają wykonawcy w takim zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.

VIII. Podstawy wykluczenia z postępowania

1. Z postępowania o udzielenie zamówienia wyklucza się wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności wskazanych:

1) w art. 108 ust. 1 ustawy PZP;
2) w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz. U. z 2024 r. poz. 507.), tj.:
   a) wymienionego w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. U. UE. L. 2006.134.1 z późn. zm.) zwanym dalej rozporządzeniem 765/2006 i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. U. UE. L. 2014.78.6 z późn. zm.), zwanym dalej rozporządzeniem 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ww. ustawy;

b) którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2024 r. poz. 1222) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ww. ustawy;

c) którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (t.j. Dz. U. z 2024 r. poz. 619 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 2022 r., 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.

IX. Podmiotowe i przedmiotowe środki dowodowe. Oświadczenia i dokumenty, jakie zobowiązani są dostarczyć Wykonawcy w celu potwierdzenia spełniania warunków udziału oraz wykazania braku podstaw wykluczenia

1. Do oferty wykonawca zobowiązany jest dołączyć aktualne na dzień składania ofert oświadczenie o spełnianiu warunków udziału w postępowaniu oraz o braku podstaw do wykluczenia z postępowania – odpowiednio zgodnie z **Załącznikiem nr 3** do SWZ.
2. Informacje zawarte w oświadczeniu, o którym mowa w ust. 1 stanowią wstępne potwierdzenie, że wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.
3. Zamawiający wzywa wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.
4. Podmiotowe środki dowodowe wymagane od wykonawcy obejmują:
   1) oświadczenie o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust 1 ustawy w zakresie podstaw wykluczeniu z postepowania – **Załącznik nr 4** do SWZ;
   2) oświadczenie własne o niepodleganiu wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego- **Załącznik nr 5** do SWZ.
5. Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*, o ile

wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy PZP dane umożliwiające dostęp do tych środków.

6. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
7. W zakresie nieuregulowanym ustawą PZP lub niniejszą SWZ do oświadczeń i dokumentów składanych przez wykonawcę w postępowaniu zastosowanie mają w szczególności przepisy Rozporządzenia Ministra Rozwoju Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. poz. 2415 z póź.zm.) oraz Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. poz. 2452).

8. Przedmiotowe środki dowodowe

   Wykonawca wraz z ofertą składa następujące przedmiotowe środki dowodowe :

   1) wypełniony formularz ***SPECYFIKACJA TECHNICZNA***, stanowiący **Załącznik nr 2.1.** do SWZ potwierdzający, że oferowany przez wykonawcę przedmiot zamówienia spełnia wymagania zamawiającego określone opisie przedmiotu zamówienia.,

   Jeżeli wykonawca nie złoży wraz z ofertą przedmiotowych środków dowodowych lub przedmiotowe środki dowodowe są niekompletne, zamawiający wezwie wykonawcę do ich złożenia lub uzupełnienia w wyznaczonym terminie. Zamawiający może żądać od wykonawcy wyjaśnień dotyczących treści przedmiotowych środków dowodowych

X. Informacje o sposobie porozumiewania się zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów

1. Postępowanie prowadzone jest w języku polskim elektronicznie za pośrednictwem platformy zakupowej pod adresem https://platformazakupowa.pl/transakcja/1100460
2. Wymaga się, aby komunikacja między zamawiającym a wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje przekazywane były za pośrednictwem platformy zakupowej i formularza „Wyślij wiadomość do zamawiającego”.

   Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformy zakupowej poprzez

kliknięcie przycisku „Wyślij wiadomość do zamawiającego” po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.

3. Zamawiający dopuszcza, awaryjnie, komunikację za pośrednictwem poczty elektronicznej ugzukowo@zukowo.pl. **Forma komunikacji za pośrednictwem poczty elektronicznej nie dotyczy złożenia oferty**.
4. Zamawiający będzie przekazywał wykonawcom informacje elektronicznie za pośrednictwem platformy zakupowej. Informacje dotyczące odpowiedzi na pytania, zmiany SWZ, zmiany terminu składania i otwarcia ofert zamawiający będzie zamieszczał na platformie zakupowej w sekcji “Komunikaty”. Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny wykonawca, będzie przekazywana w elektronicznie za pośrednictwem platformy zakupowej do konkretnego wykonawcy.
5. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformie zakupowej przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
6. Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie, określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na platformie zakupowej:

1) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
2) komputer klasy PC lub MAC o następującej konfiguracji: pamięć min 2 GB RAM, procesor Intel IV 2 GHz lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os X 10.4, Linux lub ich nowsze wersje,
3) zainstalowana dowolna przeglądarka internetowa (z wyłączeniem Internet Explorer),
4) włączona obsługa JavaScript,
5) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
6) platforma zakupowa działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,
7) oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.

7. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:

1) akceptuje warunki korzystania z platformy zakupowej określone w Regulaminie zamieszczonym na stronie internetowej pod adresem https://platformazakupowa.pl/ w zakładce „Regulamin" oraz uznaje go za wiążący,
2) zapoznał się „Instrukcjami dla wykonawców".

8. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z instrukcją korzystania z platformy zakupowej, w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego"). Taka oferta zostanie uznana przez zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu ponieważ nie został spełniony obowiązek narzucony w art. 221 ustawy PZP.
9. Zamawiający informuje, że instrukcje korzystania z platformy zakupowej dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformy zakupowej znajdują się w zakładce „Instrukcje dla wykonawców" na stronie internetowej pod adresem https://platformazakupowa.pl/strona/45-instrukcje.
10. SWZ udostępnia się na platformie zakupowej.
11. Wyjaśnienia dotyczące treści SWZ udzielane będą z zachowaniem zasad określonych w art. 284 ust. 1 - 6 ustawy PZP. Zamawiający nie przewiduje zorganizowania zebrania z wykonawcami.
12. W uzasadnionych przypadkach zamawiający może przed upływem terminu składania ofert zmienić treść SWZ. Dokonaną zmianę treści SWZ zamawiający udostępni na stronie internetowej prowadzonego postępowania.
13. Wszelkie uzupełnienia i ustalenia oraz zmiany, w tym zmiany terminów, jak również pytania wykonawców wraz z wyjaśnieniami stają się integralną częścią SWZ i będą wiążące przy składaniu ofert. Wszelkie prawa i zobowiązania wykonawcy odnośnie wcześniej ustalonych terminów będą podlegały nowemu terminowi.
14. Osoby uprawnione do komunikowania się z wykonawcami:
    1) Iwona Bujalska – sprawy formalne związane z procedurą udzielenia zamówienia publicznego,
    2) Marcin Szwarc – sprawy merytoryczne związane z przedmiotem zamówienia i jego realizacją.

XI. Opis sposobu przygotowania ofert, sposób, miejsce oraz termin składania:

1. Na ofertę składają się (dokumenty składane wraz z ofertą przez wszystkich wykonawców): wypełniony formularz ofertowy (Oferta) sporządzony z wykorzystaniem wzoru stanowiącego Załącznik nr 3 do SWZ; oświadczenie o braku podstaw do wykluczenia z postępowania oraz oświadczenie o spełnianiu

warunków udziału w postępowaniu; pełnomocnictwo (jeśli dotyczy); zobowiązanie podmiotu udostępniającego swoje zasoby wykonawcy (jeśli dotyczy); oświadczenie dotyczące realizacji zamówienia przez wykonawców wspólnie ubiegających się udzielenie zamówienia (jeśli dotyczy), dokumenty/informacje stanowiące tajemnicę przedsiębiorstwa (jeśli dotyczy).

2. Ofertę, oświadczenie o którym mowa w art. 125 ust. 1 ustawy PZP, składa się pod rygorem nieważności, w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.
   W procesie składania powyższych dokumentów na platformie zakupowej, kwalifikowany podpis elektroniczny wykonawca może złożyć bezpośrednio na dokumencie, który następnie przesyła do systemu (opcja rekomendowana przez platformę zakupową) oraz dodatkowo dla całego pakietu dokumentów w kroku 2 formularza składania oferty (po kliknięciu w przycisk „Przejdź do podsumowania").
3. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą.
4. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę upoważnioną / osoby upoważnione.
5. Poświadczenie za zgodność z oryginałem następuje w postaci elektronicznej podpisane kwalifikowanym podpisem elektronicznym /podpisem zaufanym lub podpisem osobistym przez osobę upoważnioną / osoby upoważnione.
6. Oferta powinna być:
   1) sporządzona w języku polskim,
   2) złożona przy użyciu środków komunikacji elektronicznej, tzn. za pośrednictwem platformy zakupowej,
   3) podpisana **kwalifikowanym podpisem elektronicznym** lub **podpisem zaufanym** lub **podpisem osobistym** przez osobę upoważnioną /osoby upoważnione.
7. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. *w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE*.
8. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny zamawiający wymaga dołączenia odpowiedniej ilości plików, tj. podpisywanych plików z danymi oraz plików XAdES (**wykonawca winien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym**).

9. Zamawiający zaleca, aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
10. Zgodnie z art. 18 ust. 3 ustawy PZP, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Jeżeli wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
    Na platformie zakupowej w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
11. Wykonawca, za pośrednictwem platformy zakupowej może przed upływem terminu do składania ofert zmienić lub wycofać ofertę.
    Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem https://platformazakupowa.pl/strona/45-instrukcje.
12. Cena oferty musi zawierać wszystkie koszty, jakie będzie musiał ponieść wykonawca, aby zrealizować zamówienie z najwyższą starannością oraz ewentualne rabaty.
13. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim. W przypadku załączenia dokumentów sporządzonych w innym języku, wykonawca zobowiązany jest załączyć tłumaczenie na język polski.
14. Zgodnie z definicją dokumentu elektronicznego zawartą w art. 3 pkt 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2023 r. poz. 57 z póź.zm.), opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca, albo przez podwykonawcę.
15. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.
16. Rozszerzenia plików wykorzystywanych przez wykonawców powinny być zgodne z Załącznikiem nr 2 do Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2024 r. poz. 773), zwanym dalej Rozporządzeniem KRI.

17. Zamawiający rekomenduje wykorzystanie formatów .pdf, .doc, .docx, .xls, .xlsx, .jpg, (.jpeg) **ze szczególnym wskazaniem na .pdf.**
18. W celu ewentualnej kompresji danych zamawiający rekomenduje wykorzystanie jednego z rozszerzeń .zip lub .7Z.
19. Wśród rozszerzeń powszechnych a niewystępujących w Rozporządzeniu KRI występują .rar, .gif, .bmp, .numbers, .pages. Dokumenty złożone w takich formatach zostaną uznane za złożone nieskutecznie.
20. Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi maksymalnie 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi maksymalnie 5MB.
21. W przypadku stosowania przez wykonawcę kwalifikowanego podpisu elektronicznego:
    1) ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na rozszerzenie .pdf i opatrzenie ich podpisem kwalifikowanym w formacie PAdES;
    2) pliki w innych formatach niż .pdf zaleca się opatrzyć podpisem w formacie XAdES zewnętrzny (wykonawca powinien plik z podpisem przekazywać łącznie z dokumentem podpisywanym);
    3) zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
22. Zamawiający zaleca, aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie plików różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
23. Ofertę należy przygotować z należytą starannością i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert. Zaleca się złożenie oferty na 24 godziny przed terminem składania ofert.
24. Jeśli wykonawca pakuje dokumenty np. w folder o rozszerzeniu .zip, zaleca się wcześniejsze podpisanie każdego ze skompresowanych plików.
25. Zamawiający zaleca, aby nie wprowadzać jakichkolwiek zmian w plikach po ich podpisaniu. Może to skutkować naruszeniem integralności plików i w konsekwencji będzie prowadziło do odrzucenia oferty.
26. Ofertę wraz z wymaganymi dokumentami należy umieścić na stronie internetowej prowadzonego postępowania pod adresem https://platformazakupowa.pl/transakcja/1100460 do dnia **15.05.2025 r.** do godziny **10.00**.
27. Do oferty należy dołączyć wymagane w SWZ dokumenty.

28. Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (na platformie zakupowej) w drugim kroku składania oferty poprzez kliknięcie przycisku „Złóż ofertę” i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.
29. Szczegółowa instrukcja dla wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem https://platformazakupowa.pl/strona/45-instrukcje.

XII. Otwarcie ofert

1. Otwarcie ofert następuje niezwłocznie po upływie terminu składania ofert, tj. dnia **15.05.2025 r.** o godzinie **10.15**, lecz nie później niż następnego dnia po dniu, w którym upłynął termin składania ofert.
2. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
3. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
4. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
5. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:
   1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
   2) cenach lub kosztach zawartych w ofertach.

   Powyższa informacja zostanie opublikowana na stronie postępowania https://platformazakupowa.pl/transakcja/1100460 w sekcji „Komunikaty”.

XIII. Sposób obliczania ceny oferty

1. Cena ofertowa brutto musi uwzględniać wszystkie koszty związane z realizacją przedmiotu zamówienia. Cena ofertowa jest ceną niepodlegającą negocjacji

i wyczerpującą wszelkie należności Wykonawcy wobec Zamawiającego związane z realizacją przedmiotu zamówienia.

2. Cenę oferty podaje się w złotych polskich (PLN) z dokładnością do dwóch miejsc po przecinku. Zamawiający nie przewiduje rozliczeń w walucie obcej.
3. W ofercie Wykonawca podaje cenę za realizację przedmiotu zamówienia oraz ryczałtowe ceny jednostkowe. Cenę oferty Wykonawca ustali po sporządzeniu kalkulacji ceny oferty w oparciu o Opis przedmiotu zamówienia i po doliczeniu podatku VAT. Kalkulacja ceny oferty musi być zgodna z opisem ujętym w SWZ. Wykonawca ma obowiązek podać cenę dla każdej pozycji w kalkulacji ceny.
   Ceny jednostkowe podane przez Wykonawcę w kalkulacji ceny oferty nie będą podlegały aktualizacji, pozostaną niezmienne do końca realizacji zamówienia.
4. Jeżeli została złożona oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług dla celów zastosowania kryterium ceny lub kosztu zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. W takim przypadku 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.
5. Jeżeli cena oferty będzie wydawała się rażąco niska w stosunku do przedmiotu zamówienia i budziła wątpliwości zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie w wymogami określonymi w dokumentach zamówienia lub wynikającymi z odrębnych przepisów, zamawiający

przeprowadzi postępowanie wyjaśniające zgodnie z zasadami opisanymi w art. 224 ustawy PZP. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny spoczywa na wykonawcy

6. Sposób poprawiania przez zamawiającego omyłek w obliczeniu ceny:
   1) przyjmuje się, że prawidłowo zostały podane wszystkie ceny netto oraz stawka podatku VAT.

XIV. Wymagania dotyczące wadium

Nie dotyczy

XV. Termin związania ofertą

1. Wykonawca jest związany złożoną ofertą przez okres 30 dni od dnia upływu terminu składania ofert. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

   Termin związania ofertą upływa 13.06.2025 r.

2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą wskazanego w pkt. 1, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni. Przedłużenie terminu związania ofertą wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą. Odmowa wyrażenia zgody na przedłużenie terminu związania ofertą nie powoduje utraty wadium.

XVI. Opis kryteriów oceny ofert z podaniem wag i sposobu oceny ofert

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

   a) cena - 80 %

   b) gwarancja – 20%

1. Sposób oceny ofert

Ocena ofert będzie przeprowadzona według poniższego algorytmu (wzoru):

a) **Kryterium: cena**

$C = [C_N / C_R \times 80\%] \times 100$

Oznaczenia:
C - ilość punktów badanej oferty dla kryterium cena
C_N - najniższa zaoferowana cena
C_R - cena oferty rozpatrywanej

b) **Kryterium : okres gwarancji (G)**

$G = [Go / Gmax. \times 20\%] \times 100$

gdzie: Go – gwarancja w badanej ofercie Gmax – najdłuższa gwarancja spośród ocenianych ofert.

Uwaga:
- minimalny wymagany przez Zamawiającego okres gwarancji wynosi 12 miesięcy,
- niepodanie w ofercie okresu gwarancji będzie traktowane, jako zaoferowanie 12 miesięcy,
- w przypadku podania przez Wykonawcę krótszego niż wymagany okresu gwarancji spowoduje odrzucenie oferty,
- maksymalny okres gwarancji do oceny ofert wynosi 36 miesięcy; jeżeli Wykonawca zaoferuje okres gwarancji dłuższy niż 36 miesięcy, do oceny ofert zostanie przyjęty okres 36 miesięcy,

2. Za najkorzystniejszą ofertę Zamawiający uzna ofertę, która w sumie zdobyła największą liczbę punktów. Ocenie będą podlegać wyłącznie oferty nie podlegające odrzuceniu.
3. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny lub kosztu i innych kryteriów oceny ofert, zamawiający spośród tych ofert wybiera ofertę z najniższą ceną lub najniższym kosztem, a jeżeli zostały złożone oferty o takiej samej cenie lub koszcie, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych. Oferty dodatkowe ocenia się według tych samych zasad. Wykonawcy, składając oferty

dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach.

4. Punktacja przyznawana ofertom w poszczególnych kryteriach oceny ofert będzie liczona z dokładnością do dwóch miejsc po przecinku, zgodnie z zasadami arytmetyki.
5. W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści złożonej oferty, w tym zaoferowanej ceny.
6. Zamawiający udzieli zamówienia Wykonawcy, którego oferta zostanie uznana za najkorzystniejszą.

XVII. Informacje o formalnościach, jakie powinny być dopełnione po wyborze oferty w celu zawarcia umowy

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty.
2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w pkt. 1, jeżeli w postępowaniu o udzielenie zamówienia prowadzonym w trybie podstawowym złożono tylko jedną ofertę.
3. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający zastrzega sobie prawo żądania przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych Wykonawców.
4. Wykonawca będzie zobowiązany do podpisania umowy w miejscu i terminie wskazanym przez Zamawiającego.
5. Wystąpienie którejkolwiek okoliczności związanej z działaniem lub zaniechaniem działania Wykonawcy polegającej np. na odmowie podpisania umowy na warunkach opisanych o ofercie, niestawieniu się w celu zawarcia umowy w wyznaczonym miejscu i terminie lub nie wypełnieniu obowiązków wynikających z pkt 22, traktowane będzie jako brak możliwości zawarcia umowy z przyczyn leżących po stronie Wykonawcy.

6. Przed podpisaniem umowy Wykonawca dostarcza wymagane przez zamawiającego:
   a) deklaracji zgodności CE urządzeń wydanej przez producenta urządzeń,
   b) dokument potwierdzający, że oferowany przedmiot zamówienia spełnia wymagania dyrektywy ROHS 2011/65/UE z dnia 8 czerwca 2011 r. na temat zakazu użycia niebezpiecznych substancji w wyposażeniu elektrycznym i elektronicznym (RoHS - restriction of the use of certain hazardous substances) lub spełniać warunki równoważności w postaci przedstawienia CERTYFIKATU wystawionego przez niezależną, akredytowaną jednostkę, potwierdzającego zgodność urządzeń komputerowych z dyrektywą RoHS.

XVIII. Wymagania dotyczące zabezpieczenia należytego wykonania umowy

Nie dotyczy.

XIX. Informacje o treści zawieranej umowy oraz możliwości jej zmiany

Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy: wzór umowy stanowi załącznik nr 1 do SWZ.

XX. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy

1. Środki ochrony prawnej określone w niniejszym dziale przysługują wykonawcy, uczestnikowi konkursu oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia lub nagrody w konkursie oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy PZP.
2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 PZP oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Odwołanie przysługuje na:
   1) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;

2) zaniechanie czynności w postępowaniu o udzielenie zamówienia do której zamawiający był obowiązany na podstawie ustawy;
3) zaniechanie przeprowadzenia postępowania na podstawie ustawy, mimo, że zamawiający był do tego obowiązany,

4. Odwołanie wnosi się do Prezesa Izby. Odwołujący przekazuje kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
5. Odwołanie wobec treści ogłoszenia lub treści SWZ wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub treści SWZ na stronie internetowej.
6. Odwołanie wnosi się w terminie:
   1) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
   2) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w pkt 1).
7. Odwołanie w przypadkach innych niż określone w pkt 5 i 6 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
8. Szczegółowe informacje dot. środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej” ustawy Prawo zamówień publicznych.

XXI. Spis załączników

1. Załącznik nr 1 do SWZ – Projekt umowy
2. Załącznik nr 2 do SWZ – Formularz ofertowy (***OFERTA***
3. Załącznik nr 2.1 do SWZ –Specyfikacja techniczna
4. Załącznik nr 3 do SWZ – Oświadczenie o braku podstaw do wykluczenia,
5. Załącznik nr 4 do SWZ - Oświadczenie o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust 1 ustawy w zakresie podstaw wykluczeniu z postępowania;

6. Załącznik nr 5 do SWZ - Oświadczenie własne o niepodleganiu wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

XXII. Postanowienia końcowe

W sprawach nieuregulowanych niniejszą SWZ zastosowanie mają przepisy:

1) ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych oraz aktów prawnych wydanych na jej podstawie,
2) ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny,
3) obowiązujące w zakresie przedmiotowym.