Cyberbezpieczny Samorząd

WO.271.37.2024.ZP

Krobia, dnia 31 października 2024

ZAMAWIAJĄCY:

GMINA KROBIA REPREZENTOWANA
PRZEZ BURMISTRZA

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA (SWZ)

w postępowaniu o udzielenie zamówienia publicznego prowadzonym
w trybie podstawowym na podstawie art. 275 pkt 2
o wartości zamówienia nieprzekraczającej progów unijnych o jakich stanowi art. 3 ustawy z 11 września 2019 r. - Prawo zamówień publicznych
(t. j. Dz. U. z 2024 r. poz. 1320) – dalej ustawy PZP na wykonanie zadania pn:

Poprawa Cyberbezpieczeństwa w Gminie Krobia poprzez dostawę i wdrożenie systemu przechowywania danych, oprogramowanie kopii bezpieczeństwa, klastra firewall wraz ze szkoleniem technicznym oraz przełączników sieciowych

I. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO, NUMER TELEFONU, ADRES POCZTY ELEKTRONICZNEJ ORAZ STRONY INTERNETOWEJ

GMINA KROBIA

UL. RYNEK 1

63-840 KROBIA

TEL. 65 571-11-11

FAX 65 571-11-11, 573 –87-80

REGON: 411050623

NIP: 6961749038

e-mail: projekty@krobia.pl

www.krobia.pl

REPREZENTOWANA PRZEZ: BURMISTRZA KROBI - ŁUKASZA KUBIAKA

II. ADRES STRONY INTERNETOWEJ, NA KTÓREJ UDOSTĘPNIANE BĘDĄ ZMIANY I WYJAŚNIENIA TREŚCI SWZ ORAZ INNE DOKUMENTY ZAMÓWIENIA BEZPOŚREDNIO ZWIĄZANE Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA

Postępowanie prowadzone jest w formie elektronicznej za pośrednictwem https://platformazakupowa.pl/pn/krobia.

III. TRYB UDZIELANIA ZAMÓWIENIA

Niniejsze postępowanie prowadzone jest w trybie podstawowym o jakim stanowi art. 275 pkt 2 Pzp i o wartości zamówienia nieprzekraczającej progów unijnych, o których mowa w art. 3 ustawy z 11 września 2019 r. - Prawo zamówień publicznych (t. j. Dz. U. z 2024 r. poz. 1320).

IV. INFORMACJA, CZY ZAMAWIAJĄCY PRZEWIDUJE WYBÓR NAJKORZYSTNIEJSZEJ OFERTY Z MOŻLIWOŚCIĄ PROWADZENIA NEGOCJACJI.

1. **Zamawiający może, ale nie musi, przeprowadzić negocjacji w celu ulepszenia treści ofert,** które podlegają ocenie w ramach kryteriów oceny ofert. W przypadku, gdy Zamawiający nie będzie prowadził negocjacji, dokonuje wyboru najkorzystniejszej oferty spośród niepodlegających odrzuceniu ofert złożonych w odpowiedzi na ogłoszenie o zamówieniu.
2. Zamawiający nie korzysta z uprawnienia, o jakim stanowi art. 288 ust. 1 Ustawy.
3. W przypadku podjęcia przez Zamawiającego decyzji o przeprowadzeniu negocjacji w celu ulepszenia treści ofert, do negocjacji Zamawiający zaprosi wszystkich Wykonawców, którzy w odpowiedzi na ogłoszenie o zamówieniu złożyli oferty niepodlegające odrzuceniu - w pierwszym kroku zamawiający poinformuje równocześnie wszystkich wykonawców, którzy złożyli oferty, o wykonawcach:
   1) których oferty nie zostały odrzucone oraz punktacji przyznanej ofertom w każdym kryterium oceny ofert i łącznej punktacji,
   2) których oferty zostały odrzucone - podając uzasadnienie faktyczne i prawne.
4. W przypadku podjęcia przez Zamawiającego decyzji o prowadzeniu negocjacji, Zamawiający **zaprasza jednocześnie wszystkich Wykonawców**, **którzy w odpowiedzi na ogłoszenie o zamówieniu złożyli oferty niepodlegające odrzuceniu.**
5. W zaproszeniu do negocjacji Zamawiający wskazuje:
   1) miejsce prowadzenia negocjacji,
   2) termin prowadzenia negocjacji,
   3) sposób prowadzenia negocjacji,
   4) kryteria oceny ofert w ramach których będą prowadzone negocjacje w celu ulepszenia treści ofert.
6. Podczas negocjacji ofert Zamawiający zapewnia równe traktowanie wszystkich Wykonawców.
7. Zamawiający nie udziela informacji w sposób, który mógłby zapewnić niektórym Wykonawcom przewagę nad innymi Wykonawcami.
8. Prowadzone negocjacje mają charakter poufny.

9. Żadna ze stron nie może, bez zgody drugiej strony, ujawniać informacji technicznych i handlowych związanych z negocjacjami. Zgoda jest udzielana w odniesieniu do konkretnych informacji i przed ich ujawnieniem.
10. Zamawiający informuje równocześnie wszystkich Wykonawców, których oferty złożone w odpowiedzi na ogłoszenie o zamówieniu nie zostały odrzucone **(oznacza to Wykonawców, którzy zostali zaproszeni do negocjacji, nawet jak w tych negocjacjach nie brali udziału)**, o zakończeniu negocjacji oraz zaprasza ich do składania ofert dodatkowych **(udział Wykonawców w negocjacjach nie jest konieczny, ale zaproszenie do składania ofert dodatkowych zostanie przesłane do wszystkich Wykonawców, których oferty nie zostały odrzucone, nawet jeśli nie brali oni udziału w negocjacjach).**
11. Zaproszenie do składania ofert dodatkowych zawiera co najmniej:
1) nazwę oraz adres Zamawiającego, numer telefonu, adres poczty elektronicznej oraz strony internetowej prowadzonego postępowania,
2) sposób i termin składania ofert dodatkowych oraz język lub języki, w jakich muszą być one sporządzone oraz termin otwarcia tych ofert.
12. Wykonawca może złożyć ofertę dodatkową, która zawiera nowe propozycje **w zakresie treści oferty podlegających ocenie w ramach kryteriów oceny ofert wskazanych przez Zamawiającego w zaproszeniu do negocjacji. W przypadku, gdy Wykonawca nie złoży oferty dodatkowej, wówczas wiążąca będzie oferta złożona w odpowiedzi na ogłoszenie o zamówieniu.**
13. Oferta dodatkowa nie może być mniej korzystna w żadnym z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu.
14. Oferta przestaje wiązać Wykonawcę w takim zakresie, w jakim złoży on ofertę dodatkową zawierającą korzystniejsze propozycje w ramach każdego z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji.
15. **Oferta dodatkowa, która jest mniej korzystna** w którymkolwiek z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu, **podlega odrzuceniu.**

V. OPIS PRZEDMIOTU ZAMÓWIENIA

Poprawa Cyberbezpieczeństwa w Gminie Krobia poprzez dostawę i wdrożenie systemu przechowywania danych, oprogramowanie kopii bezpieczeństwa, klastra firewall wraz ze szkoleniem technicznym oraz przełączników sieciowych

Zamówienie realizowane w ramach projektu grantowego Cyberbezpieczna Gmina Krobia Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1329/ FERC.02.02-CS.01-001/23/2024 realizowanego w ramach konkursu grantowego „Cyberbezpieczny Samorząd".

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego pn. „Cyberbezpieczny Samorząd", Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC)

Oznaczenie przedmiotu zamówienia wg wspólnego słownika zamówień CPV

48820000- 2 Serwery
31122000-7 Jednostki prądotwórcze
32422000-7 Elementy składowe sieci
32420000-3 Urządzenia sieciowe
48000000-8 Pakiety oprogramowania i systemy informatyczne
30230000-0 Sprzęt związany z komputerami
72263000-6 Usługi wdrażania oprogramowania
72541000-9 Usługi rozbudowy sprzętu komputerowego

Opis Przedmiotu zamówienia:

1. **System do przechowywania danych :**
   1.1. Macierz dyskowa – 1 sztuka wraz z wdrożeniem.

Wdrożenie obejmuje:

- Instalację dostarczonej macierzy w szafie rack

- Podłączenie macierzy do infrastruktury LAN Zamawiającego
- Konfigurację sieci SAN (iSCSI)
- Udostępnienie wolumenów do dostarczonych serwerów.
- Sprawdzenie poprawności działania, obejmujące m. in. symulację awarii pojedynczego dysku oraz pojedynczego kontrolera.

LP.	Funkcjonalność
1.	Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowana macierz nie może przekroczyć rozmiaru 2U. Obudowa musi umożliwiać instalację min. 24 dysków.
2.	Oferowane urządzenie musi być przystosowane do zasilania z sieci AC oraz wyposażone w kable zasilające PDU. Macierz musi być wyposażona w zdublowany, redundantny system zasilania, umożliwiający prawidłową, nieprzerwaną pracę urządzenia w przypadku awarii dowolnego pojedynczego źródła zasilania.
3.	Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active-active. Architektura symmetric active-active. Praca kontrolerów w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek i portów kontrolerów bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery nie mogą pracować w trybie active-passive.
4.	Macierz w oferowanej konfiguracji w teście wydajnościowym osiągnie min. 100 000 IOPS przy następujących parametrach: • Zapełnienie macierzy – min. 75% fizycznej pojemności, • Protokół: iSCSI, • Porty: 10Gb, • Read 80% - blok 8k, • Write 20% - blok 8k, • 100% Random • Read Hit Ratio – 0% • Write Hit Ratio – 0% • Latency – max. 1ms

	• RAID 6 Zamawiający ma prawo przeprowadzić test po dostawie macierzy aby sprawdzić, czy dostarczone rozwiązanie osiąga deklarowane parametry wydajnościowe.
5.	Fizyczna przestrzeń dyskowa zbudowana za pomocą dysków SSD SAS. Przestrzeń użytkowa po zbudowaniu RAID 6 z 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności 1 dysku, musi wynosić min 16 TB. Ze względów wydajnościowych oraz niezawodnościowych rozmiar pojedynczego dysku nie może być większy niż 4 TB. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń spare i dostępna dla hostów bez uwzględnienia mechanizmów kompresji, czy deduplikacji. Dyski muszą być wyposażone w podwójne interfejsy. Niedopuszczalne są dyski SSD zbudowane w oparciu o technologię QLC.
6.	Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.
7.	Rozbudowa oferowanej macierzy, do co najmniej 98 dysków SSD SAS, bez wymiany kontrolerów macierzowych oraz bez rozbudowy o dodatkowe kontrolery, tylko poprzez dodawanie półek i dysków SSD SAS.
8.	Co najmniej 128GB pamięci cache na całą macierz (dwa kontrolery). Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć.
9.	Razem kontrolery muszą udostępnić minimum 12 portów 10Gb Eth. Wymagana możliwość rozbudowy o dodatkowe 8 portów 10Gb Eth lub 8 portów 16G FC bez konieczności wymiany lub zakupu nowych kontrolerów i klastrowania z kontrolerami oferowanymi w tym postępowaniu. Wszystkie moduły muszą posiadać wkładki optyczne SFP+. Macierz musi posiadać wbudowane min. 4 porty SAS 12Gb/s do podłączenia półek dyskowych.

10.	Wymagane wsparcie dla protokołów iSCSI. Wsparcie dla protokołu FC po rozbudowie macierzy o interfejsy FC.
11.	Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków bez utraty danych.
12.	Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Macierz musi wspierać nie mniej niż 1024 LUNów. Wymagana możliwość tworzenia grup wolumenów. Max. liczba LUNów w grupie wolumenów nie może być mniejsza niż 100.
13.	Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy w tym monitorowanie wydajności obiektów takich jak: • cała macierz • kontrolery • porty front-end • dyski • LUNy • hosty Pod kątem parametrów takich jak: • operacje wejścia/wyjścia IOPS • przepustowość (KB/s lub MB/s) • czas odpowiedzi (latency) Wymagana możliwość monitorowania stanu żywotności dysków SSD SAS. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Wymagana możliwość konfigurowania zasobów macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest

	wymagane na tym etapie postępowania.
14.	Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych. Snapshoty muszą być wykonywanie w technologii ROW (Redirect On Write). Macierz musi obsługiwać min 2000 snapshotów. Wymagane wsparcie dla snapshotów kaskadowych. Wymagana możliwość tworzenia harmonogramu wykonywania snapshotów oraz zabezpieczenia migawek przed modyfikacją lub usunięciem pod kątem szybkiego przywrócenia danych w przypadku ataku ransomware. Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model macierzy. Tworzenie na żądanie kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z wolumenu źródłowego na docelowy oraz resynchronizację danych z wolumenu docelowego na źródłowy. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
15.	Macierz musi wspierać funkcjonalności deduplikacji i kompresji danych w trybie in-line (w locie). Musi być możliwe włączenie deduplikacji i kompresji per wolumen (LUN). Musi istnieć możliwość wyłączenia tych funkcjonalności na wybranych wolumenach (LUN). Dostarczenie licencji na tę funkcjonalność jest wymagane na tym etapie postępowania.
16.	Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybie asynchronicznym oraz synchronicznym przy wykorzystaniu portów FC lub IP. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
17.	Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage

	Metro Cluster). Macierz musi dostarczać funkcjonalność klastra klasy "wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform oprogramowania i sprzętowych z wykorzystaniem synchronicznej replikacji danych po protokole FC lub IP pomiędzy 2 macierzami. Pod użytym pojęciem "wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy (macierz preferowana) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodujących dla danego środowiska brak dostępu do zasobów macierzy preferowanej. Funkcjonalność klastra "wysokiej dostępności" pozwala na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy preferowanej na niepreferowaną w przypadku awarii macierzy preferowanej (tzw. automated failover). Wymagany jest również automatyczny failover z macierzy niepreferowanej na preferowaną. Dopuszczalne jest zastosowanie tzw arbitra (serwer quorum). Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
18.	Macierz musi posiadać możliwość zapewnienia ciągłości biznesu na oczekiwanym poziomie usług (QoS) poprzez definicję polityk QoS w oparciu o maksymalne progi wydajności IOPS i MB/s. Musi istnieć możliwość określenia polityk QoS na poziomie wolumenów. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
19.	Macierz musi oferować wsparcie dla zachowania integralności danych na całej ścieżce transferu (ang. End-to-End) zgodnego ze standardem/specyfikacją T10 PI.
20.	Wsparcie, dla co najmniej Microsoft Server Windows 2016/2019/2022, VMware 7.x/8.x, Linux RedHat 7.x/8.x, CentOS 7.x/8.x
21.	Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania. Macierz musi umożliwiać zdalne zarządzanie. Urządzenie musi być

	fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP. Wymagana gwarancja 3 lata w trybie 9x5 NBD.

1.2. **Serwer – 2 sztuki wraz z wdrożeniem**.

Wdrożenie obejmuje:

- Montaż serwerów w szafie rack.
- Instalację środowiska wirtualizującego (VMware lub równoważne)
- Konfigurację sieci w środowisku VMware lub równoważnym
- Podłączenie współdzielonych zasobów dyskowych udostępnionych z dostarczonej macierzy dyskowej.
- Konfigurację klastra HA.
- Sprawdzenie poprawności działania klastra HA.
- Migrację maszyn wirtualnych oraz fizycznych wskazanych przez Zamawiającego do zainstalowanego środowiska wirtualnego.

LP.	Funkcjonalność
1.	Obudowa: a. Typu RACK, wysokość maksymalnie 1U b. Szyny umożliwiające wysunięcie serwera z szafy wraz z ramieniem porządkującym kable z tyłu obudowy c. Możliwość zainstalowania 8 dysków twardych hot-plug 2,5” d. Zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych e. Zainstalowane 2 dyski 2,5” SSD SATA 960GB hot-plug skonfigurowane w RAID1
2.	Płyta główna: a. Jednoprocesorowa b. Wyprodukowana i zaprojektowana przez producenta serwera c. Możliwość instalacji procesorów 128-rdzeniowych

	d. Zainstalowany moduł TPM 2.0 e. Minimum 3 fizyczne złącza PCI Express generacji 5 o prędkości x16 f. Minimum 24 gniazda pamięci RAM g. Obsługa minimum 6 TB pamięci RAM DDR5 h. Możliwość instalacji 2 dysków M.2 na płycie głównej
3.	Procesor: a. Zainstalowany jeden procesor 16-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem b. Minimum 178 punktów w teście SPECrate®2017_int_base, dostępnym na stronie www.spec.org dla proponowanego serwera c. Taktowanie bazowe minimum 3.0 GHz d. Minimum 64 MB pamięci podręcznej L3
4.	Pamięć RAM: a. Minimum 192 GB pamięci RAM b. DDR5 RDIMM 4800 MT/s c. Pamięci obsadzone w sposób gwarantujący najwyższą możliwość wydajność d. Możliwość podwojenia ilości pamięci bez konieczności wymiany zainstalowanych modułów
5.	Kontrolery LAN: a. Dwie dwuportowe karty 10Gbit SFP+ nie zajmujące żadnego z dostępnych slotów PCI Express b. Możliwość zamiany kart 10Gbit SFP+ na dwie dwuportowe karty 100Gbit QSFP28 bez konieczności zajmowania slotów PCIe
6.	Kontrolery I/O: a. Kontroler SAS RAID dla dysków wewnętrznych, obsługujący poziomy RAID: 0,1,10
7.	Porty a. Zintegrowana karta graficzna ze złączem VGA z tyłu i z przodu serwera b. Minimum 2 porty USB 3.2 dostępne z tyłu serwera c. Minimum 2 porty USB 3.2 na panelu przednim

	d. Możliwość zainstalowania portu szeregowego (RS-232-C), możliwość wykorzystania portu szeregowego do zarządzania serwerem e. Liczba dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących złącza PCI Express i/lub USB serwera
8.	Zasilanie, chłodzenie: a. Redundantne zasilacze hot-plug o sprawności 96% (tzw. klasa Titanium) o mocy 900W b. Redundantne wentylatory hot-plug
9.	Zarządzanie a. Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii b. informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: • karty rozszerzeń zainstalowanej w dowolnym slocie PCI Express • procesory CPU • pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM • wbudowany na płycie głównej nośnik pamięci M.2 SSD • status karty zarządzającej serwera • wentylatory • bateria podtrzymująca ustawienia BIOS płyty głównej • zasilacze • system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym) c. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego

	zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie w tym zdalny restart serwera • Dedykowana karta LAN 1 Gb/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym • Dostęp poprzez: przeglądarkę WWW, SSH • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Obsługa VLAN • Wsparcie dla protokołu SSDP • Obsługa protokołów TLS 1.3, SSL v3 • Obsługa protokołu LDAP • Synchronizacja czasu poprzez protokół NTP • Możliwość wykonywania kopii bezpieczeństwa ustawień bios serwera oraz ustawień karty zarządzającej d. Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna) e. Dedykowana pamięć flash dająca możliwość zdalnej reinstalacji

	systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN f. Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej
10.	Wspierane systemy operacyjne: a. Microsoft Windows Server 2022 b. VMWare vSphere 7, 8 c. Suse Linux Enterprise Server 15 d. Red Hat Enterprise Linux 9, 8 e. Oracle Linux 9, 8
11.	Gwarancja a. 3 lata gwarancji producenta serwera w trybie onsite z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis b. Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu c. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych d. Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniony w ofercie e. Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.

12.	Dokumentacja, inne: a. Elementy, z których zbudowany jest serwer muszą być produktami producenta serwera lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta b. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta c. Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera d. W czasie obowiązywania gwarancji, możliwość sprawdzenia, po podaniu na infolinii numeru seryjnego urządzenia, pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typu udzielonej gwarancji e. Zgodność z normami: CB, RoHS, WEEE oraz CE
13.	Wraz z serwerami należy dostarczyć licencję na 1. 4 x Windows Server 2022 Standard. Każda z licencji odpowiednia dla liczby rdzeni w zaoferowanym procesorze. 2. Wraz z serwerami należy dostarczyć licencję na VMware Standard . Licencja odpowiednia dla liczby rdzeni w zaoferowanych serwerach na okres 2 lat.

2. Przełącznik sieciowy typ 1 – 2 sztuki wraz z wdrożeniem.

Wdrożenie obejmuje:

- Montaż przełączników w szafie rack
- Konfigurację interfejsów zarządzających
- Konfigurację sieci VLAN
- Konfigurację sieci SAN (iSCSI)
- Podłączenie dostarczonej macierzy dyskowej oraz serwerów
- Podłączenie przełączników do infrastruktury Zamawiającego

LP.	Funkcjonalność
1.	Urządzenie musi być wyposażone w minimum 24 porty 10Gigabit Ethernet SFP+, 6 portów 40Gigabit Ethernet QSFP28 mogących pracować jako 100Gigabit Ethernet QSFP28 po instalacji dodatkowej licencji.
2.	Urządzenie musi być dostarczone z 1m DAC QSFP+ 40Gb, 4 x SFP+ 10Gb SR, 4 x SFP 1Gb RJ45;
3.	Urządzenie musi umożliwiać stworzenie wirtualnego systemu - złożonego z min. 2 przełączników szkieletowych będących przedmiotem opisu - zarządzanego jako jedno urządzenie logiczne. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać połączenie w system z wykorzystaniem standardowych portów 10Gigabit Ethernet / 40 Gigabit Ethernet Ethernet oraz modułów optycznych lub kabli DAC. Musi istnieć możliwość terminowania połączeń link aggregation na dwóch przełącznikach tworzących taki system wirtualny (tzw. multi-chassis link aggregation)
4.	Urządzenie musi być wyposażone w wewnętrzne redundantne zasilacze 230V AC wspierające mechanizm HotSwap.
5.	Urządzenie musi być wyposażone w wewnętrzne redundantne wentylatory wspierające mechanizm HotSwap.
6.	Przepływ powietrza musi odbywać się od strony portów (zasysanie) w kierunku zasilaczy i modułów wentylacyjnych (wydmuch).
7.	Wymagane parametry wydajnościowe: a. Switching capacity: minimum 1 600 Gbps b. Forwarding capacity: minimum 480 Mpps c. min. 380 000 wpisów w tablicy adresów MAC d. min. 140 000 wpisów w tablicy ARP e. min. 190 000 wpisów w tablicy routingowej IPv4 f. min. 80 000 wpisów w tablicy routingowej IPv6 g. min. 60 000 tras multicast h. min. 6 000 wpisów na potrzeby realizacji polityk bezpieczeństwa (listy kontroli dostępu ACL) i. min. 1 000 interfejsów VLAN

	j. min. 4 094 aktywnych sieci VLAN
8.	Obsługa protokołów warstwy 3 dla IPv4: Open Shortest Path First (OSPF), BGPv4, ISIS-IPv4
9.	Obsługa protokołów warstwy 3 dla IPv6: Open Shortest Path First (OSPFv3), BGP+, ISIS-IPv6
10.	Obsługuje protokoły multicastowe w tym PIM Sparse i Dense Mode, SSM, IGMP/MLD
11.	Obsługuje protokoły MPLS, LDP, L2 i L3 VPN, VPLS, MPLS TE, MPLS.
12.	Musi umożliwiać rozbudowę o funkcjonalność VxLAN w przyszłości poprzez np.: zakup licencji
13.	Urządzenie wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: a. IEEE 802.1w Rapid Spanning Tree b. IEEE 802.1s Multiple Spanning Tree c. IEEE 802.3ad (Link Aggregation Control Protocol) umożliwiający grupowanie portów.
14.	Urządzenie wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci (QoS): a. Obsługa min. 8 kolejek per port, w tym co najmniej jedna kolejka ze statusem strict priority b. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP c. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP d. Definiowanie polityk QoS per port i per VLAN
15.	Urządzenie wspiera następujące mechanizmy związane z bezpieczeństwem: a. Wiele poziomów dostępu administracyjnego poprzez konsolę -

	autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend b. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1X z możliwością przydziału listy kontroli dostępu (ACL) i VLANu c. Obsługa co najmniej następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard d. Weryfikacja źródła pakietu względem tablicy routingu (uRPF) – zarówno dla IPv4 i IPv6 e. Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP f. Listy kontroli dostępu także dla IPv6 g. Mechanizmy ochrony warstwy kontrolnej
16.	Obsługuje ramki Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame)
17.	Urządzenie przystosowane do montażu w szafie 19”, wysokość nie większa niż 1RU, elementy niezbędne do montażu muszą być dostarczone z urządzeniem
18.	Urządzenie musi wspierać następujące mechanizmy związane z zarządzaniem: a. Ma możliwość zarządzania przez WEB Gui (HTTPS), SNMPv3 oraz SSHv2 b. Umożliwia zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Ethernet out-of-band management c. Umożliwia identyfikację i uwierzytelnianie w oparciu o serwer RADIUS lub TACACS+ d. Posiada port USB e. Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie (SPAN,RSPAN), polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN f. Posiada możliwość raportowania do systemów zarządzających z

	wykorzystaniem statystyk typu flow (J-Flow, NetFlow, sFlow lub odpowiednik). g. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych
19.	Urządzenie musi być wyposażone w zintegrowany kontroler sieci WLAN zdolny do pracy w klastrze HA przy utworzeniu stosu przełączników.
20.	Wbudowany serwer DHCP obsługujący co najmniej 64 pule adresów IP
21.	Obsługa funkcji DHCP klient i DHCP relay
22.	Obsługa funkcji: ochrony serwera DHCP, DHCP snooping, Dynamic ARP Inspection, IP Source Guard
23.	Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
24.	Obsługa 802.3ad Link Aggregation Protocol (LACP)
25.	Funkcja BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom
26.	Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
27.	Obsługa routingu statycznego i dynamicznego (co najmniej protokoły: RIP, OSFP, ISIS, BGP)
28.	Obsługa routingu bazującego na politykach (Policy Based Routing)
29.	Obsługa IGMP v1/v2/v3 oraz IGMP snooping i IGMP proxy
30.	Obsługa protokołu PIM-SM
31.	Funkcja izolacji użytkowników radiowych (wewnątrz grupy a także pomiędzy grupami użytkowników)
32.	Funkcja automatycznego zwiększania mocy pobliskich AP w przypadku awarii jednego z nich w celu zapewnienia pełnego pokrycia sygnałem WiFi

33.	Obsługa sieci IEEE 802.1Q VLAN – minimum 4 000 sieci VLAN obsługiwanych równocześnie
34.	Zarządzanie poprzez wbudowane Web GUI jak i możliwe zarządzanie przy pomocy zewnętrznego serwera z Web GUI
35.	Zarządzanie poprzez port konsoli (CLI)
36.	Wsparcie dla SNMP v1/v2/v3
37.	Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
38.	Wymagany jest serwis gwarancyjny świadczony przez minimum 3 lata. Dostępność serwisu 9x5xNBD. W trakcie trwania serwisu zapewniony dostęp do poprawek i nowych wersji oprogramowania
39.	Gwarantowany czas naprawy sprzętu – 48h od momentu zgłoszenia i potwierdzenia awarii.

3. Przełącznik sieciowy typ 2 – 2 sztuki wraz z wdrożeniem.

Wdrożenie obejmuje:

- Montaż przełączników w szafie rack
- Konfigurację interfejsów zarządzających
- Konfigurację sieci VLAN
- Podłączenie przełączników do infrastruktury Zamawiającego
- Podłączenie urządzeń końcowych do dostarczonych przełączników

LP.	Funkcjonalność
1.	Urządzenie musi być wyposażone w minimum 48 portów 10BASE-T/100BASE-TX/1000BASE-T ze wsparciem dla trybów: full-duplex, half-duplex, automatycznej negocjacji (auto-negotiation).
2.	Urządzenie musi być wyposażone w minimum 4 porty 1/10Gb SFP/SFP+, pozwalające na instalację wkładek 10Gb (SFP+), Gigabitowych (SFP) oraz kabli DAC/Twinax SFP+.
3.	Urządzenie musi być dostarczone z modułami SFP+ w następującej konfiguracji: 4 sztuki 10G SR, 1 przewód DAC SFP+ o długości 1m
4.	Urządzenie musi umożliwiać stworzenie wirtualnego systemu - złożonego z min. 8 przełączników zarządzanego jako jedno urządzenie logiczne. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać połączenie w

	system z wykorzystaniem standardowych portów 10Gigabit Ethernet oraz modułów optycznych lub kabli DAC. Musi istnieć możliwość terminowania połączeń link aggregation na dwóch przełącznikach tworzących taki system wirtualny (tzw. multi-chassis link aggregation)
5.	Urządzenie musi być wyposażone w wewnętrzne redundantne zasilacze 230V AC wspierające mechanizm HotSwap.
6.	Wymagane parametry wydajnościowe: a. Switching capacity: minimum 176 Gbps b. Forwarding capacity: minimum 125 Mpps c. min. 64 000 wpisów w tablicy adresów MAC d. min. 16 000 wpisów w tablicy ARP e. min. 32 000 wpisów w tablicy routingu IPv4 f. min. 8 000 wpisów w tablicy routingu IPv6 g. min. 2 000 wpisów na potrzeby realizacji polityk bezpieczeństwa (listy kontroli dostępu ACL) h. min. 1 000 interfejsów VLAN i. min. 4 094 aktywnych/jednoczesnych sieci VLAN
7.	Obsługa protokołów warstwy 3 dla IPv4: Open Shortest Path First (OSPF), BGPv4, ISIS-IPv4
8.	Obsługa protokołów warstwy 3 dla IPv6: Open Shortest Path First (OSPFv3), BGP4+, ISIS-IPv6
9.	Obsługuje protokoły multicastowe w tym PIM Sparse i Dense Mode, SSM, IGMP/MLD
10.	Urządzenie wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: a. IEEE 802.1w Rapid Spanning Tree b. IEEE 802.1s Multiple Spanning Tree c. IEEE 802.3ad (Link Aggregation Control Protocol) umożliwiający grupowanie portów.
11.	Urządzenie wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci (QoS): a. Obsługa min. 8 kolejek per port, w tym co najmniej jedna kolejka ze

	statusem strict priority b. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP c. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP d. Definiowanie polityk QoS per port i per VLAN
12.	Urządzenie wspiera następujące mechanizmy związane z bezpieczeństwem: a. Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend b. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1X z możliwością przydziału listy kontroli dostępu (ACL) i VLANu c. Obsługa co najmniej następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard d. Weryfikacja źródła pakietu względem tablicy routingu (uRPF) – zarówno dla IPv4 i IPv6 e. Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP f. Listy kontroli dostępu także dla IPv6 g. Mechanizmy ochrony warstwy kontrolnej
13.	Obsługuje ramki Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame)
14.	Przystosowane do montażu w szafie 19”, wysokość nie większa niż 1RU, elementy niezbędne do montażu muszą być dostarczone z urządzeniem
15.	Urządzenie musi wspierać następujące mechanizmy związane z zarządzaniem: a. Ma możliwość zarządzania przez WEB Gui (HTTPS), SNMPv3 oraz

	SSHv2 b. Umożliwia zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Ethernet out-of-band management c. Umożliwia identyfikację i uwierzytelnianie w oparciu o serwer RADIUS lub TACACS+ d. Posiada port USB e. Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie (SPAN,RSPAN), polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN f. Posiada możliwość raportowania do systemów zarządzających z wykorzystaniem statystyk typu flow (J-Flow, NetFlow, sFlow lub odpowiednik) g. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych
16.	Wymagany jest serwis gwarancyjny świadczony przez minimum 3 lata. Dostępność serwisu 9x5xNBD. W trakcie trwania serwisu zapewniony dostęp do poprawek i nowych wersji oprogramowania

4. System zarządzający kopią bezpieczeństwa wraz z wdrożeniem.

Wdrożenie obejmuję:

a. Instalacja systemu na udostępnionym przez Zamawiającego serwerze fizycznym.
b. Instalację niezbędnych komponentów wymaganych do poprawnej konfiguracji zadań kopii bezpieczeństwa.
c. Konfiguracja zadań kopii bezpieczeństwa zgodnie z najlepszymi praktykami.
d. Konfiguracja dostarczonej przez Zamawiającego biblioteki taśmowej.
e. Konfiguracja kopii bezpieczeństwa na dostarczoną przez Zamawiającego bibliotekę taśmową.

f. Konfiguracja automatycznego, cyklicznego zadania testowego odtwarzania wskazanych przez Zamawiającego systemów wraz z generowaniem raportów z wykonania zadania.

LP.	Funkcjonalność
1.	Wymagania ogólne a. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Dostarczona licencja musi być licencją wieczystą ze wsparciem minimum 1 rok. Dostarczona licencja musi pozwalać na ochronę minimum 40 maszyn wirtualnych. b. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x i 8.x oraz Microsoft Hyper-V 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej c. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
2.	Całkowite koszty posiadania a. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej b. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków c. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji d. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być

	przechowywane w plikach backupu. e. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych w takiej puli. f. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. g. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. h. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania i. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) j. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu k. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API l. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji m. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji

	n. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania o. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. p. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej q. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora) r. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS) s. Oprogramowanie musi posiadać integracje z systemami typu SIEM t. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.
3.	Wymagania RPO a. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej b. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. c. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru d. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia

	jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. e. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. f. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). g. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) h. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, Quantum DXi i. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. j. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. k. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. l. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO. m. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik n. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji

	(replica seeding) o. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
4.	Wymagania RTO a. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. b. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) c. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami d. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre e. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. f. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków g. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack,

	Amazon EC2 oraz Google Cloud Platform. h. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików i. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. j. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell k. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM l. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. m. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. n. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt, w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. o. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. p. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych

	witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. q. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. r. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. s. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji t. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN u. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle v. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI w. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2 x. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
5.	Ograniczenie ryzyka a. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) b. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

	c. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem d. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. e. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware f. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania g. Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków h. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
6.	Środowiska fizyczne a. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego b. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych c. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE d. Rozwiązanie musi wspierać system operacyjny macOS

	e. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix f. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również scentralizowany (poprzez centralną konsolę zarządzającą) g. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster h. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów i. Rozwiązanie musi wspierać backup podłączonych dysków USB j. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym k. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) l. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone m. Rozwiązanie musi wspierać kontrolę pasma sieciowego n. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych o. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN p. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft q. Rozwiązanie musi wspierać technologię BitLocker

	r. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania s. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2016 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych t. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych u. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. v. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform w. Rozwiązanie musi wspierać szyfrowanie x. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne y. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego z. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej aa. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

5. Klaster firewall- System UTM – 2 sztuki wraz z wdrożeniem.

Wdrożenie obejmuje:

a. Instalację dostarczonych systemów w infrastrukturze Zamawiającego.
b. Konfigurację klastra HA active-active

c. Odtworzenie konfiguracji z posiadanych przez Zamawiającego systemów FG300D oraz Stormshield na zainstalowanym systemie
d. Konfigurację polityk bezpieczeństwa
e. Konfigurację połączeń VPN
f. Konfigurację routingu
g. Po przeprowadzanej instalacji i konfiguracji wymagane jest przeszkolenie administratora z całości systemu UTM ze szczególnym uwzględnieniem nowych funkcjonalności.

LP.	Funkcjonalność
1.	Wymagania Ogólne a. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. b. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. c. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. d. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
2.	Redundancja, monitoring i wykrywanie awarii

	a. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. b. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. c. Monitoring stanu realizowanych połączeń VPN. d. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3.	Interfejsy, Dysk, Zasilanie: a. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 16 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 2 gniazdami SFP+ 10 Gbps. b. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. c. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. d. System jest wyposażony w zasilanie AC.
4.	Parametry wydajnościowe: a. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. b. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. c. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B. d. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.

	e. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. f. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps. g. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps. h. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. i. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
5.	Funkcje Systemu Bezpieczeństwa: W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. b. Kontrola Aplikacji. c. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. d. Ochrona przed malware. e. Ochrona przed atakami - Intrusion Prevention System. f. Kontrola stron WWW. g. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. h. Zarządzanie pasmem (QoS, Traffic shaping). i. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). j. 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. k. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

	l. Analiza ruchu szyfrowanego protokołem SSH. m. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. n. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
6.	Polityki, Firewall a. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. b. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. c. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. d. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. e. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. f. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7.	Połączenia VPN a. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługę protokołu Diffie-Hellman grup 19, 20 oraz 21.

	• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Dynamiczne zestawianie tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. b. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
8.	Funkcje SD-WAN a. System umożliwia wykorzystanie protokołów dynamicznego routingu

	przy konfiguracji równoważenia obciążenia do łączy WAN. b. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). c. Reguły SD-WAN umożliwiają określenie aplikacji jako argumentu dla kierowania ruchu. d. Rozwiązanie powinno wspierać funkcję Forward Error Correctionm na tunelach IPSec. e. Funkcja monitorowania łącza w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.
9.	Zarządzanie pasmem a. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. b. System daje możliwość określania pasma dla poszczególnych aplikacji. c. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. d. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
10.	Ochrona przed malware a. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). b. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, SMTP, CIFS. c. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. d. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. e. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co

	najmniej dla systemu operacyjnego Android). f. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. g. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. h. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. i. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. j. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
11.	Ochrona przed atakami a. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. b. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. c. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. d. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. e. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. f. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). g. Możliwość kontrolowania długości nagłówka, liczby parametrów URL oraz Cookies dla protokołu http. h. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

	i. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
12.	Kontrola aplikacji a. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. b. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. c. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. d. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. e. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. f. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). g. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
13.	Kontrola WWW a. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. b. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. c. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. d. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

	e. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). f. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. g. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. h. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. i. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. j. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. k. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla serwisów: youtube, vimeo. l. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.
14.	Uwierzytelnianie użytkowników w ramach sesji a. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. b. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. c. System umożliwia budowę architektury uwierzytelniania typu Single

	Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. d. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
15.	Zarządzanie a. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. b. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. c. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. d. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. e. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. f. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. g. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. h. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). i. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
16.	Logowanie a. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne

	jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. b. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. c. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. d. Możliwość włączenia logowania per reguła w polityce firewall. e. System zapewnia możliwość logowania do serwera SYSLOG. f. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
17.	Serwisy i licencje Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: a. 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 12 miesięcy.
18.	Gwarancja oraz wsparcie a. System jest objęty serwisem gwarancyjnym producenta przez okres 12 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.
19.	Rozszerzone wsparcie serwisowe AHB/SOS a. System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez

	okres 12 miesięcy. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: • Wsparcie telefoniczne zespołu certyfikowanych inżynierów. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. • Doradztwo w zakresie konfiguracji. • Zdalne wsparcie techniczne. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta. • Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). • Przygotowanie urządzenia do zdalnej konfiguracji. • Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. • Wsparcie techniczne wymaganego serwisu. • Należy posiadać Certyfikat ISO 9001 podmiotu serwisującego.
20.	Voucher na szkolenie dla administratora autoryzowane przez producenta rozwiązania, certyfikat wydany przez producenta potwierdzający odbycie szkolenia, czas trwania min:4 dni, voucher do wykorzystania przez 12 m-cy

6. Zasilacz awaryjny UPS – 1 szt

W skład zasilacza wchodzi:

Zasilacz awaryjny UPS przystosowany do montażu w szafach typu rack 19” wraz z uchwytami montażowymi do szaf rack 19” oraz zestawem przewodów zasilających oraz sygnałowych.

Do protokołu odbioru należy dołączyć karty katalogowe lub działające linki do strony internetowej producenta, które prowadzą do kart katalogowych zasilacza awaryjnego UPS.

LP.	Funkcjonalność	
1.	Moc wyjściowa: 8000W / 8000VA.	
2.	Napięcie wyjściowe: 230V.	
3.	Maksymalna możliwa do konfiguracji moc: 8000W / 8000VA.	
4.	Zniekształcenie harmoniczne: mniej niż 3%.	
5.	Częstotliwość na wyjściu (synchronicznie z siecią): 57–63Hz przy częstotliwości nominalnej 60Hz.	
6.	Topologia: Podwójna konwersja (online).	
7.	Typ przebiegu: sinusoida.	
8.	Gniazda wyjściowe: a. IEC 320 C13 - 6 sztuk, b. IEC 320 C19 - 4 sztuki, c. IEC Jumpers - 3 sztuki.	
9.	Nominalne napięcie wejściowe: 230V / 400V	
10.	Częstotliwość na wejściu: 40/70Hz (automatyczne wykrywanie).	
11.	Typ gniazda wejściowego: połączenie poprzez zacisk 3-przewodowy.	
12.	Inne napięcia wejściowe: 220V, 240V.	
13.	Limit napięcia wejściowego: 140V - 275V.	
14.	Typ akumulatora: bezobsługowy akumulator kwasowo-ołowiowy.	
15.	Typowy czas pełnego ładowania akumulatora: 2 godziny.	
16.	Oczekiwana żywotność akumulatora: 3 - 5 lat.	
17.	Czas podtrzymania dla obciążenia 100%: minimum 5 minut.	
18.	Czas podtrzymania dla obciążenia 50%: minimum 14 minut.	
19.	Możliwość podłączenia zewnętrznych modułów bateryjnych.	
20.	Port komunikacyjny: UPS wyposażony w kartę do zdalnego	

	zarządzania z gniazdem RJ45.	
21.	Panel przedni: wielofunkcyjna konsola sterownicza i informacyjna LCD.	
22.	Obudowa: przystosowana do mocowania w szafie RACK 19”, dostarczona wraz z szynami umożliwiającymi montaż urządzenia w szafie RACK 19”.	
23.	Maksymalna wysokość: 6U.	
24.	Temperatura pracy: 0 °C - 40 °C.	
25.	Wilgotność względna podczas pracy: 0% - 95%.	
26.	Temperatura (przechowywanie): -15 °C - +45 °C,	
27.	Potwierdzenia zgodności: CE, VDE, IRAM, EN/IEC 62040-1:2019/A11:2021, EN/IEC 62040-2:2006/AC:2006, EN/IEC 62040-2:2018.	
28.	Okres gwarancji: minimum 2 lata gwarancji na zasilacz oraz 2 lata na moduły bateryjne.	

W ramach niniejszego postępowania Zamawiający wymaga podłączenia, skonfigurowania i uruchomienia zaoferowanego urządzenia UPS do sieci elektrycznej Urzędu celem zabezpieczenia pomieszczenia serwerowni. Wszystkie koszty z tym związane np.: modernizacji istniejącej instalacji elektrycznej muszą zostać przewidziane i uwzględnione w ofercie Wykonawcy.

7. Zasilacz awaryjny UPS – 6 szt

Do protokołu odbioru należy załączyć karty katalogowe lub działające linki do strony internetowej producenta, które prowadzą do kart katalogowych zasilacza awaryjnego UPS.

LP.	Nazwa komponentu	Wymagania minimalne
1.	Moc pozorna	1400 0VA
2.	Moc rzeczywista	700 VA
3.	Napięcie znamionowe	230 V

4.	Częstotliwość znamionowa	50 Hz
5.	Kształt napięcia	Sinusoidalny
6.	Napięcie znamionowe wyjściowe	230 V
7.	Częstotliwość wyjściowa	50 Hz
8.	Typ obudowy	Wolnostojący
9.	Wyposażenie	UPS, instrukcja obsługi (może być w postaci elektronicznej), instrukcja bezpieczeństwa. - 1 x kabel komunikacyjny USB 1 x kabel zasilający - wejściowy

Wymagania pozostałe:

1. Dostarczone sprzęty i oprogramowanie muszą być kompletne i muszą posiadać wszelkie wymagane instrukcje, gwarancje i licencje.

2. Oferta musi być jednoznaczna i kompleksowa, tj.: obejmować cały asortyment proponowanego przedmiotu zamówienia Przedmiot zamówienia musi być kompletny, ze wszystkimi podzespołami, częściami i materiałami niezbędnymi do uruchomienia i użytkowania sprzętu zgodnie z jego przeznaczeniem. Oferowany przedmiot zamówienia musi spełniać wymogi Zamawiającego.

3. Wykonawca może zaoferować sprzęt o parametrach nie gorszych lub lepszych niż opisane, jednak w żadnym stopniu nie obniżający standardu i nie zmieniający rozwiązań technicznych podanych w OPZ, a tym samym nie pozbawiający Zamawiającego żądanych wydajności, funkcjonalności, użyteczności opisanego sprzętu. Wskazanie przez Zamawiającego w SWZ marek lub nazw handlowych towarów ma charakter wyłącznie przykładowy, pomocniczy dla określenia klasy produktu, a nie wskazuje na konkretny wyrób lub konkretnego producenta. Wykonawca przy sporządzeniu oferty kieruje się wyłącznie wymaganiami co do parametrów towarów, a nie ma obowiązku oferowania towarów podanych jako przykładowe. W przypadku zaoferowania oprogramowania równoważnego, na wykonawcy spoczywa obowiązek udowodnienia, że

uprawnienia Zamawiającego wynikające z posiadanych przez niego licencji oraz cechy oferowanego oprogramowania są równoważne w stosunku do oprogramowania określonego w OPZ. W tym celu wykonawca zobowiązany jest załączyć do oferty opis i dane techniczne zaproponowanego rozwiązania, umożliwiające porównanie go z wszystkimi parametrami, wymaganymi opisem przedmiotu zamówienia, w tym zgodność posiadanego przez Zamawiającego oprogramowania z zaproponowanym rozwiązaniem. Wykonawca w razie potrzeby może zadać Zamawiającemu pytanie o posiadane licencje, oprogramowania i sprzęt - wyłącznie w celu i w zakresie niezbędnym do prawidłowego sporządzenia oferty.
W przypadku, gdy zaoferowane przez wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego, również po odinstalowaniu oprogramowania równoważnego.

4. Oprogramowanie musi być zaoferowane w najnowszych, obecnie dostępnych wersjach.

5. Dostawa przedmiotu zamówienia odbywać się będzie na koszt i ryzyko wykonawcy na miejsce wskazane przez Zamawiającego. Urządzenia dostarczane będą bez plombowanych obudów z oznakowanymi podzespołami głównymi z możliwością instalacji rozszerzeń bez utraty gwarancji. Z chwilą dostarczenia przedmiotu zamówienia przejdą na Zamawiającego korzyści i ciężary związane z przedmiotem zamówienia oraz niebezpieczeństwo jego przypadkowej utraty lub uszkodzenia. Sprzęt ma być dostarczony w oryginalnych opakowaniach producenta.

6. Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.

7. Dla oprogramowania musi być publicznie znany cykl życia przedstawiony przez producenta systemu i dotyczący rozwoju wsparcia technicznego – w szczególności w zakresie bezpieczeństwa. Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych bezpłatnie przez producenta na jego stronie internetowej w okresie co najmniej 5 lat.

8. Zamawiający wymaga, aby wszystkie elementy oprogramowania biurowego oraz jego licencja pochodziły od tego samego producenta.

9. Urządzenia będące przedmiotem zamówienia muszą być fabrycznie nowe, nieużywane, w pełni sprawne i wolne od wad fizycznych. Przedmiot umowy nie może być obciążony prawami osób trzecich.

10. Cały sprzęt musi mieć kompletne odpowiednie okablowanie niezbędne do uruchomienia poszczególnych urządzeń.

11. Wszystkie elementy określone w opisie przedmiotu zamówienia muszą stanowić integralną część urządzeń. Zamawiający nie dopuszcza możliwości konfigurowania sprzętu za pomocą elementów zewnętrznych, za wyjątkiem sytuacji, gdy opis przedmiotu zamówienia wyraźnie na to wskazuje

12. Wszystkie urządzenia objęte zamówieniem muszą być fabrycznie nowe, w możliwie najwyższej klasie jakości, nieużywane, nieregenerowane, kompletne, wyprodukowane nie wcześniej niż w styczniu 2023 r. oraz dostarczone w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished”.

13. Oprogramowanie objęte zamówieniem musi być nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej najwyższej stabilnej wersji i pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych. Zamawiający zastrzega możliwość przeprowadzenia weryfikacji oryginalności dostarczonego oprogramowania u Producenta w przypadku wystąpienia wątpliwości co do jego legalności.

Odbiór przedmiotu umowy:

Zamawiający dokona odbioru przedmiotu umowy w przeciągu 14 dni od zgłoszenia gotowości do odbioru na podstawie zgodności z Opisem Przedmiotu Zamówienia w formie uzgodnionej z wykonawcą.

Zamawiający nie dopuszcza odbioru częściowego zamówienia,
Wykonawca ponosi wszystkie koszty związane z dostarczeniem przedmiotu umowy do Zamawiającego oraz odpowiada za przedmiot umowy (ryzyko utraty, uszkodzenia itd.) do czasu jego odbioru przez Zamawiającego

Gwarancja:

a) min. 36 miesięcy na sprzęt wymieniony w pkt. 1 , 2, 3
b) 24 miesiące na sprzęt wymieniony w pkt. 6,7
c) 12 miesięcy na sprzęt wymieniony w pkt. 5

Fakturowanie i płatności:

1. Podstawą wystawienia faktury będzie podpisany ze strony Zamawiającego protokół zdawczo-odbiorczy podpisany przez strony umowy.
2. Zamawiający nie dopuszcza fakturowania częściowego podczas realizacji zamówienia
3. Zamawiający nie przewiduje płatności w 2024 r.
4. Termin płatności faktury 14 dni

Brak podziału na części spowodowany jest specyfiką przedmiotu zamówienia, jego skomplikowaniem i wieloetapowością, co przy założeniu podziału na części prowadziłoby do powstania trudności organizacyjnych i logistycznych, technicznych oraz groziłby nadmiernymi kosztami wykonania zamówienia .

VI. TERMIN WYKONANIA ZAMÓWIENIA

77 dni od podpisania umowy

VII. PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI TEJ UMOWY

1. Zamawiający wymaga, aby wybrany Wykonawca zawarł z nim umowę na warunkach określonych w projekcie umowy stanowiącym załącznik do SWZ.

2. Zamawiający, zgodnie z art. 455 ustawy Pzp, przewiduje możliwość dokonania zmian postanowień zawartej umowy w sprawie zamówienia publicznego, w sposób i na warunkach określonych w projekcie umowy.

VIII. INFORMACJE O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI, ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ

Zgodnie z art. 61 ust. 1 ustawy Pzp komunikacja w niniejszym postępowaniu w tym składanie ofert, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń między Zamawiającym a Wykonawcą odbywa się przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 o świadczeniu usług drogą elektroniczną za pośrednictwem Platformy Zakupowej.

1. Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem https://platformazakupowa.pl/pn/krobia.

2. W celu skrócenia czasu udzielenia odpowiedzi na pytania preferuje się, aby komunikacja między Zamawiającym a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane były za pośrednictwem https://platformazakupowa.pl/pn/krobia i formularza „Wyślij wiadomość do zamawiającego".

Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem https://platformazakupowa.pl/pn/krobia poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego" po których pojawi się komunikat, że wiadomość została wysłana do Zamawiającego. Zamawiający dopuszcza, awaryjnie, komunikację za pośrednictwem poczty elektronicznej. Adres poczty

elektronicznej osoby uprawnionej do kontaktu z Wykonawcami: projekty@krobia.pl

3. Zamawiający będzie przekazywał wykonawcom informacje w formie elektronicznej za pośrednictwem https://platformazakupowa.pl/pn/krobia. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w sekcji “Komunikaty”. Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny Wykonawca, będzie przekazywana w formie elektronicznej za pośrednictwem https://platformazakupowa.pl/pn/krobia do konkretnego Wykonawcy.
4. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na https://platformazakupowa.pl/pn/krobia przesłanych przez Zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
5. Zamawiający, zgodnie z § 11 ust. 2 Rozporządzenia Prezesa Rady Ministrów 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. 2020 poz. 2452) określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na https://platformazakupowa.pl/pn/krobia, tj.:
    a) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
    b) 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,
    c) zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10 0.,
    d) włączona obsługa JavaScript,
    e) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,

f) https://platformazakupowa.pl/pn/krobia działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,

g) 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.

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

a) akceptuje warunki korzystania z https://platformazakupowa.pl/pn/krobia określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący,

b) zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej pod linkiem.

7. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z https://platformazakupowa.pl/pn/krobia, 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.

8. Zamawiający informuje, że instrukcje korzystania z https://platformazakupowa.pl/pn/krobia dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu https://platformazakupowa.pl/pn/krobia znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.

IX. INFORMACJE O SPOSOBIE KOMUNIKOWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI W INNY SPOSÓB NIŻ PRZY UŻYCIU ŚRODKÓW KOMUNIKACJI ELEKTRONICZNEJ W PRZYPADKU ZAISTNIENIA JEDNEJ Z SYTUACJI OKREŚLONYCH W ART. 65 UST. 1, ART. 66 I ART. 69

Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.

X. WSKAZANIE OSÓB UPRAWNIONYCH DO KOMUNIKOWANIA SIĘ Z WYKONAWCAMI

Osobą uprawnioną do kontaktu z wykonawcami jest:

Judyta Ratajczak
stanowisko – ZAMÓWIENIA PUBLICZNE I ENERGETYKA GMINNA
od poniedziałku do piątku w siedzibie Zamawiającego, w pokoju nr 5, w godzinach (poniedziałek $8^{\underline{00}}$ -$16^{\underline{00}}$, wtorek – piątek $7^{\underline{00}}$ -$15^{\underline{00}}$)

XI. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca będzie związany ofertą przez okres **30 dni**, tj. **DO DNIA 12 grudnia 2024 r.** Bieg terminu związania ofertą rozpoczyna się w dniu, w którym upływa termin składania ofert.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, 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 **(art. 307 ust. 2 i 3 Pzp).**

XII. OPIS SPOSOBU PRZYGOTOWANIA OFERT

1. Oferta, wniosek oraz przedmiotowe środki dowodowe (jeżeli były wymagane) składane elektronicznie muszą zostać podpisane elektronicznym kwalifikowanym podpisem lub podpisem zaufanym lub podpisem osobistym. Zamawiający wyjaśnia, że wszystkie wymienione rodzaje podpisu, włącznie z podpisem osobistym, **są podpisami elektronicznymi, a nie własnoręcznymi.** W procesie składania oferty, wniosku w tym przedmiotowych środków dowodowych na platformie, kwalifikowany podpis elektroniczny, podpis zaufany lub podpis osobisty, Wykonawca może złożyć

bezpośrednio na dokumencie, który następnie przesyła do systemu (**opcja rekomendowana** przez https://platformazakupowa.pl/pn/krobia)
oraz dodatkowo dla całego pakietu dokumentów w kroku 2 **Formularza składania oferty lub wniosku** (po kliknięciu w przycisk **Przejdź do podsumowania**).

2. Oferta musi być podpisana przez Wykonawcę lub osoby uprawnione do reprezentacji Wykonawcy w obrocie gospodarczym, zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze i wymogami ustawowymi, bądź osobę (osoby) właściwie umocowane. Jeżeli oferta zostanie podpisana przez inną osobę lub osoby, do oferty należy dołączyć stosowne pełnomocnictwo lub pełnomocnictwa do reprezentacji dla tych osób.
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. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione, 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 (Dz. U. z 2020r. poz. 2452).
4. Oferta powinna być:
   a) sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
   b) złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem https://platformazakupowa.pl/pn/krobia,

c) podpisana **kwalifikowanym podpisem elektronicznym** lub **podpisem zaufanym** lub **podpisem osobistym** przez osobę/osoby upoważnioną/upoważnione.

5. Podpisy kwalifikowane wykorzystywane przez Wykonawców do podpisywania wszelkich plików muszą spełniać wymogi wynikające z "Rozporządzenia Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku".
6. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej liczby plików tj. podpisanych plików z danymi oraz plików XAdES.
7. Zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
8. Wykonawca, za pośrednictwem https://platformazakupowa.pl/pn/krobia 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
9. Każdy z Wykonawców może złożyć tylko jedną ofertę. Oferta złożona przez Wykonawcę musi obejmować całość zamówienia. **Treść złożonej przez Wykonawcę oferty musi być zgodna z wymaganiami Zamawiającego określonymi w dokumentach zamówienia oraz ustawą Pzp (art. 218 ust. 2 Pzp).**
10. Ceny oferty muszą zawierać wszystkie koszty, jakie musi ponieść Wykonawca, aby zrealizować zamówienie z najwyższą starannością.
11. Oferta winna być przygotowana na formularzu oferty stanowiącym **załącznik do niniejszej specyfikacji** bądź zawierać wszystkie dane wymienione we

wzorze formularza ofertowego. Wykonawca jest zobowiązany do podania prawidłowych danych adresowych Wykonawcy wynikających z właściwego rejestru (np. KRS, CEIDG).

12. Do oferty winny być dołączone wszystkie dokumenty wymagane postanowieniami zawartymi w niniejszej SWZ. Wszystkie opracowane przez Zamawiającego załączniki - druki do niniejszej specyfikacji stanowią wyłącznie propozycje co do formy wymaganych dokumentów. Dopuszcza się przedstawienie wymaganych załączników w formie własnej opracowanej przez Wykonawcę, pod warunkiem, iż dokumenty będą zawierać wszystkie żądane przez Zamawiającego informacje zawarte w załącznikach i niniejszej specyfikacji oraz będą podpisane przez uprawnionego przedstawiciela do reprezentacji w obrocie gospodarczym Wykonawcy.

13. Dokumenty i oświadczenia składane przez Wykonawcę powinny być w języku polskim, chyba że w SWZ dopuszczono inaczej. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, Wykonawca zobowiązany jest załączyć tłumaczenie na język polski.

14. Zgodnie z definicją dokumentu elektronicznego z art.3 ust. 2 Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, 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 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych”, zwanego 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:
    a) .zip
    b) .7Z
19. Wśród rozszerzeń powszechnych a **niewystępujących** w Rozporządzeniu KRI występują: .rar .gif .bmp .numbers .pages. **Dokumenty złożone w takich plikach 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:
    - 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.**
    - Pliki w innych formatach niż PDF **zaleca się opatrzyć podpisem w formacie XAdES o typie zewnętrznym**. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
    - 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 różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.**
23. Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.

24. Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. **Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.**

25. Jeśli Wykonawca pakuje dokumenty np. w plik o rozszerzeniu .zip, zaleca się wcześniejsze podpisanie każdego ze skompresowanych plików.

26. Zamawiający zaleca aby **nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty.**

27. **NA OFERTĘ SKŁADAJĄ SIĘ NASTĘPUJĄCE DOKUMENTY:**

a) Formularz ofertowy, zgodnie z **załącznikiem nr 1 do SWZ,**

b) Oświadczenie o spełnianiu warunków udziału w postępowaniu - zgodnie z **załącznikiem nr 2 do SWZ** – **w przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie składane jest przez Wykonawcę wykazującego spełnienie warunku,**

c) Oświadczenie o niepodleganiu wykluczeniu z postępowania, zgodnie z **załącznikiem nr 3 do SWZ – w przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie o niepodleganiu wykluczenia składa każdy z Wykonawców,**

d) Dokument potwierdzający, że Wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia ze wskazaniem sumy gwarancyjnej tego ubezpieczenia, **jako załącznik nr 4 (nie należy dołączać do oferty – składa Wykonawca, którego oferta zostanie najwyżej oceniona),**

e) Wykaz dostaw wykonanych nie wcześniej niż w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich rodzaju, wartości, daty i miejsca wykonania oraz podmiotów, na rzecz których dostawy te zostały wykonane, oraz załączeniem dowodów określających, czy te dostawy zostały wykonane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a jeżeli wykonawca z przyczyn niezależnych od niego

nie jest w stanie uzyskać tych dokumentów – inne odpowiednie dokumenty, według wzoru stanowiącego załącznik **nr 5 do SWZ** **(nie należy dołączać do oferty – składa Wykonawca, którego oferta zostanie najwyżej oceniona),**

f) Pełnomocnictwo upoważniające do złożenia oferty, o ile ofertę składa pełnomocnik,

g) Pełnomocnictwo do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienie – dotyczy ofert składanych przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia (nie dotyczy spółki cywilnej, o ile upoważnienie/pełnomocnictwo do występowania w imieniu tej spółki wynika z dołączonej do oferty umowy spółki bądź wszyscy wspólnicy podpiszą ofertę),

h) Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia określające, które dostawy wykonują poszczególni Wykonawcy - **według wzoru stanowiącego załącznik nr 6 do SWZ** – w przypadku wspólnego ubiegania się o zamówienie przez Wykonawców,

i) Zobowiązanie podmiotu udostępniającego zasoby **według wzoru stanowiącego załącznik nr 7 do SWZ** - jeżeli Wykonawca w celu potwierdzenia spełnienia warunków udziału polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby wraz z zobowiązaniem składa oświadczenie o niepodleganiu wykluczeniu z postępowania tego podmiotu oraz oświadczenie o spełnianiu warunków udziału w postępowaniu w zakresie, w jakim Wykonawca powołuje się na jego zasoby.

XIII. SPOSÓB ORAZ TERMIN SKŁADANIA OFERT

1. Ofertę wraz z wymaganymi dokumentami należy umieścić na platformie zakupowej pod adresem: https://platformazakupowa.pl/pn/krobia do dnia **13.11.2024** r. **do godziny 8:00**.

Uwaga:

ZA DATĘ I GODZINĘ ZŁOŻENIA OFERTY ROZUMIE SIĘ DATĘ I GODZINĘ JEJ WPŁYWU NA PLATFORMĘ PRZETARGOWĄ, TJ. DATĘ I GODZINĘ ZŁOŻENIA OFERTY WYŚWIETLONĄ NA KONCIE ZAMAWIAJĄCEGO

2. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty.

3. Po wypełnieniu Formularza składania oferty i dołączeniu wszystkich wymaganych załączników należy kliknąć przycisk **„Przejdź do podsumowania”.**
4. Oferta składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem https://platformazakupowa.pl/pn/krobia, Wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem https://platformazakupowa.pl/pn/krobia. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust 1 oraz ust. 2 Pzp, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust.1 sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio w odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
5. **Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku “Złóż ofertę” i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.**
6. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.
7. Wykonawca po upływie terminu do składania ofert nie może wycofać złożonej oferty.

XIV. TERMIN OTWARCIA OFERT

1. Otwarcie ofert nastąpi w dniu **13.11.2024** r. **o godzinie 8:30.**
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 **(art. 222 ust. 2 Pzp).**

3. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania **(art. 222 ust. 3 Pzp).**
4. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia **(art. 222 ust. 4 Pzp).**
5. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o **(art. 222 ust. 5 Pzp)** :
   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.
   Informacja zostanie opublikowana na stronie postępowania na https://platformazakupowa.pl/pn/krobia w sekcji ,,Komunikaty" .

Uwaga! Zgodnie z Ustawą Pzp **Zamawiający nie ma obowiązku przeprowadzania jawnej sesji otwarcia ofert** w sposób jawny z udziałem Wykonawców lub transmitowania sesji otwarcia za pośrednictwem elektronicznych narzędzi do przekazu wideo on-line, a ma jedynie takie uprawnienie.

XV. PODSTAWY WYKLUCZENIA Z POSTĘPOWANIA

1. Z postępowania o udzielenie zamówienia wyklucza się (z zastrzeżeniem art. 110 ust. 2 Pzp) Wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności wskazanych **w art. 108 ust. 1 Pzp:**

1.1. Wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:

a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,

b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,

c) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2023 r. poz. 2048 oraz z 2024 r. poz. 1166) lub w art. 54 ust. 1-4 ustawy z dnia 12 maja 2011 r. o

refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2024 r. poz. 930)

d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,

e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,

f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 1745),

g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d Kodeksu karnego lub przestępstwo skarbowe,

h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej – lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

1.2. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;

1.3. wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne

lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

1.4. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;

1.5. jeżeli Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;

1.6. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego Wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

2. Zamawiający **nie przewiduje** podstaw wykluczenia, o których mowa **w art. 109 ust. 1 Pzp.**

3. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.

4. Wykluczenie wykonawcy z postępowania następuje w przypadkach i na zasadach określonych szczegółowo w art. 111 ustawy Pzp, z zastrzeżeniem art.110 ust. 2 ustawy Pzp.

5. Z postępowania o udzielenie zamówienia wyklucza się Wykonawcę w przypadkach, o których mowa 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 (Dz.U. 2024 poz. 507).

Do Wykonawcy podlegającego wykluczeniu w tym zakresie, stosuje się art. 7 ust. 3 wspomnianej ustawy, z którego wynika, że z postępowania o udzielenie zamówienia wyklucza się:

1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3;
2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124, 1285, 1723 i 1843) 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;
3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598) 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.

XVI. INFORMACJA O WARUNKACH UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy **(art. 57 Pzp) nie podlegają wykluczeniu na zasadach określonych w niniejszej SWZ, oraz spełniają określone przez Zamawiającego warunki udziału w postępowaniu.**
2. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki udziału **(art. 112 Pzp)** dotyczące:
   1) **zdolności do występowania w obrocie gospodarczym:**
      Zamawiający nie stawia warunku w powyższym zakresie.
   2) **uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:**
      Zamawiający nie stawia warunku w powyższym zakresie.

3) **sytuacji ekonomicznej lub finansowej:**
O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy są ubezpieczeni od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia z sumą gwarancyjną tego ubezpieczenia w wysokości 500 000,00 zł.

4) **zdolności technicznej lub zawodowej:** Wykonawca spełni warunek zdolności technicznej, jeżeli wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie należycie i prawidłowo przeprowadził co najmniej 1 dostawę i wdrożenie sprzętu serwerowego i/lub macierzy dyskowej za kwotę co najmniej 200 tys. zł brutto (w ramach jednego zadania), wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane, oraz z załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie.

3. WYKONAWCY WSPÓLNIE UBIEGAJĄCY SIĘ O UDZIELENIE ZAMÓWIENIA.

1) Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia (art. 58 ust. 1 Pzp).
2) Podmioty występujące wspólnie ponoszą solidarną odpowiedzialność za niewykonanie lub nienależyte wykonanie zamówienia.
3) Wykonawcy wspólnie ubiegający się o udzielenie zamówienia, ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego – nie dotyczy spółki cywilnej, o ile

upoważnienie/pełnomocnictwo do występowania w imieniu tej spółki wynika z dołączonej do oferty umowy spółki bądź wszyscy wspólnicy podpiszą ofertę.

4) Przepisy Prawa zamówień publicznych dotyczące Wykonawcy stosuje się odpowiednio do Wykonawców wspólnie ubiegających się o zamówienia.
5) Warunek dotyczący uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o którym mowa w art. 112 ust. 2 pkt 2 ustawy Pzp, jest spełniony, jeżeli co najmniej jeden z Wykonawców wspólnie ubiegających się o udzielenie zamówienia posiada uprawnienia do prowadzenia określonej działalności gospodarczej lub zawodowej i zrealizuje roboty budowlane, dostawy lub usługi, do których realizacji te uprawnienia są wymagane **(art. 117 ust. 2 Pzp).**

W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane **(art. 117 ust. 3 Pzp).**

W przypadku, o którym mowa w niniejszym punkcie, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia **dołączają** do oferty **oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni Wykonawcy, zgodnie z załącznikiem nr 6 do SWZ (art. 117 ust. 4 Pzp).**

W odniesieniu do warunków określonych **w rozdziale XVI SWZ**, wymagania te muszą być spełnione wspólnie przez Wykonawców składających ofertę w postępowaniu **(nie musi ich spełniać osobno każdy z Wykonawców składających ofertę wspólną)**. Na ich potwierdzenie należy złożyć dokumenty określone **w rozdziale XVII SWZ.**

Każdy z Wykonawców występujących wspólnie **zobowiązany jest do wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia publicznego.** W takim przypadku oświadczenia i/lub dokumenty wymienione w **rozdziale XVII SWZ** składa każdy z Wykonawców występujących

wspólnie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia **(art.125 ust. 4 Pzp).**

4. PODWYKONAWCY

1) Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy **(art. 462 ust. 1 Pzp).**
2) Wykonawca, który zamierza wykonywać zamówienie przy udziale podwykonawcy/ów, musi wyraźnie w ofercie wskazać, jaką część (zakres zamówienia) wykonywać będzie w jego imieniu podwykonawca **oraz podać nazwę ewentualnych podwykonawców**, **jeżeli są już znani**.
3) Zamawiający żąda, aby przed przystąpieniem do wykonania zamówienia Wykonawca podał nazwy, dane kontaktowe oraz przedstawicieli, podwykonawców zaangażowanych w wykonanie zamówienia (jeżeli są już znani). Wykonawca zobowiązany jest do zawiadomienia Zamawiającego o wszelkich zmianach w odniesieniu do informacji, o których mowa w zdaniu pierwszym, w trakcie realizacji zamówienia, a także przekazuje wymagane informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację zamówienia.
4) Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.
5) Jeżeli Wykonawca powierzył wykonanie części zamówienia podwykonawcy **i podwykonawca ten nie jest podmiotem udostępniającym zasoby**, Zamawiający nie bada, czy zachodzą wobec tego podwykonawcy podstawy wykluczenia, o których mowa w art. 108 i art. 109 ustawy PZP oraz w swz.
6) Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 118 ust. 1 ustawy Pzp, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać zamawiającemu, że proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby

Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia **(art. 462 ust. 7 Pzp.).**

Przepis art. 122 ustawy Pzp stosuje się odpowiednio.

XVII. INFORMACJA O PODMIOTOWYCH ŚRODKACH DOWODOWYCH

1. Do oferty Wykonawca zobowiązany jest dołączyć **na dzień składania ofert** oświadczenie o spełnianiu warunków udziału w postępowaniu oraz o braku podstaw do wykluczenia z postępowania **(art. 273 ust. 2 i art.125 ust.3 Pzp)** – zgodnie z **załącznikiem nr 2 i 3 do SWZ oraz pozostałe dokumenty wskazane w rozdziale XII pkt 27 SWZ (należy dołączyć do oferty).**
2. Zamawiający **NIE ŻĄDA** złożenia podmiotowych środków dowodowych **NA POTWIERDZENIE BRAKU PODSTAW WYKLUCZENIA** wykonawcy z udziału w postępowaniu.
3. Zamawiający **ŻĄDA** złożenia podmiotowych środków dowodowych **NA POTWIERDZENIE SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU.**
4. Zamawiający wzywa wykonawcę **(274 ust. 1 Pzp)**, którego oferta **została najwyżej oceniona**, do złożenia w wyznaczonym terminie, **nie krótszym niż 5 dni od dnia wezwania**, podmiotowych środków dowodowych, jeżeli wymagał ich złożenia w ogłoszeniu o zamówieniu lub dokumentach zamówienia, **aktualnych na dzień złożenia podmiotowych środków dowodowych. (aktualnych na dzień złożenia)**
5. Podmiotowe środki dowodowe wymagane od wykonawcy obejmują:
   W zakresie wykazania spełnienia przez Wykonawcę warunków udziału w postępowaniu dotyczących sytuacji ekonomicznej lub finansowej należy przedłożyć, na wezwanie Zamawiającego, dokument potwierdzający, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia ze wskazaniem sumy gwarancyjnej tego ubezpieczenia, **jako załącznik nr 4 – (nie należy dołączać do oferty – składa Wykonawca, którego oferta zostanie najwyżej oceniona)**.

W zakresie wykazania spełnienia przez Wykonawcę warunków udziału w postępowaniu dotyczącej zdolności technicznej lub zawodowej należy przedłożyć, na wezwanie Zamawiającego:

Wykaz, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie należycie i prawidłowo przeprowadził Dostawę i wdrożenie sprzętu serwerowego i/lub macierzy dyskowej za kwotę 200 tys. zł brutto, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane, oraz z załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie - według wzoru stanowiącego załącznik nr 5 do SWZ, Wyżej wskazany okres 3 lat liczy się wstecz od dnia w którym upływa termin składania ofert **(nie należy dołączać do oferty – składa Wykonawca, którego oferta zostanie najwyżej oceniona).**

6. Wykonawcy, którzy mają siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, składają dokumenty na zasadach opisanych w Rozporządzeniu Ministra Rozwoju, Pracy i Technologii w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia.

7. 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 Pzp dane umożliwiające dostęp do tych środków **(art. 274 ust. 4 Pzp) .**

8. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność **(art. 127 ust. 2 Pzp).**

9. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu lub są one niekompletne lub zawierają błędy, Zamawiający wzywa Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie, chyba że:
1) oferta Wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub
2) zachodzą przesłanki unieważnienia postępowania **(art. 128 ust. 1 Pzp)**.

10. Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp lub złożonych podmiotowych środków dowodowych lub innych dokumentów lub oświadczeń składanych w postępowaniu **(art. 128 ust. 4 Pzp)**.

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 w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać Zamawiający od Wykonawcy oraz rozporządzenia Prezesa Rady Ministrów 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.

UWAGA:
JEŻELI ZACHODZĄ UZASADNIONE PODSTAWY DO UZNANIA, ŻE ZŁOŻONE UPRZEDNIO PODMIOTOWE ŚRODKI DOWODOWE NIE SĄ JUŻ AKTUALNE, ZAMAWIAJĄCY MOŻE W KAŻDYM CZASIE WEZWAĆ WYKONAWCĘ LUB WYKONAWCÓW DO ZŁOŻENIA WSZYSTKICH LUB NIEKTÓRYCH PODMIOTOWYCH ŚRODKÓW DOWODOWYCH, AKTUALNYCH NA DZIEŃ ICH ZŁOŻENIA (ART. 274 UST. 3 P.Z.P).

XVIII. INFORMACJA O PRZEDMIOTOWCH ŚRODKACH DOWODOWYCH

Zamawiający **nie wymaga złożenia przedmiotowych środków dowodowych.**

XIX. SPOSÓB OBLICZENIA CENY

1. Wykonawca podaje cenę za realizację całości przedmiotu zamówienia zgodnie ze wzorem formularza ofertowego, stanowiącego załącznik nr 1 do SWZ. Cenę należy ustalić na podstawie kalkulacji własnej, biorąc pod uwagę przedmiot zamówienia.
2. Za cenę oferty uważać się będzie cenę brutto podaną w formularzu ofertowym.
3. Podana cena w formularzu ofertowym jest ceną ryczałtową i nie podlega zmianom z zastrzeżeniem warunków opisanych we wzorze umowy.
4. Cena ryczałtowa brutto musi zawierać ostateczną, sumaryczną cenę realizacji przedmiotu zamówienia obejmującą wszystkie koszty (z uwzględnieniem wszystkich opłat i podatków) związane z realizacją przedmiotu zamówienia zgodnie z opisem przedmiotu zamówienia oraz istotnymi postanowieniami umowy określonymi w niniejszej SWZ. Stawka podatku VAT w przedmiotowym postępowaniu wynosi 23 %.
5. Cena oferty powinna być wyrażona w złotych polskich (PLN) z dokładnością do dwóch miejsc po przecinku.
6. Zamawiający nie przewiduje rozliczeń w walucie obcej.
7. Wyliczona cena oferty brutto będzie służyć do porównania złożonych ofert i do rozliczenia w trakcie realizacji zamówienia.
8. 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 (Dz. U. z 2024 r. poz. 361), 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 ofercie 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 (art. 225 ust. 1 i ust. 2 Pzp).

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

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

- CENA **znaczenie – 60 %**

- DODATKOWY OKRES GWARANCJI **znaczenie – 40 %**

Kryterium „CENA" – ocenie zostanie poddana cena brutto oferty za realizację całości zamówienia, obliczona przez wykonawcę, podana w „FORMULARZU OFERTOWYM". Maksymalną liczbę punktów, tj. 60 pkt otrzyma Wykonawca, który zaproponuje najniższą cenę brutto, pozostali natomiast proporcjonalnie mniej. Oceny pozostałych ofert zostaną przeliczone według następującego wzoru:

$$\text{Ocena} = \frac{\text{Cena brutto najniższej zaproponowanej oferty}}{\text{Cena brutto oferty badanej}} \times 60$$

Kryterium „DODATKOWY OKRES GWARANCJI":

Ocenie zostanie poddany wydłużony termin gwarancji dla przedmiotu zamówienia opisanego w pkt. 1,2,3 opisu przedmiotu zamówienia.

Zgodnie z informacjami zawartymi w Opisie Przedmiotu Zamówienia:
Podstawowy okres Gwarancji na sprzęt wymieniony w pkt. 1 , 2, 3 wynosi 36 miesięcy

W przypadku zaoferowania gwarancji dla punktów 1.2.3 OPZ – 36 miesięcy zamawiający przyzna – 0 pkt.
W przypadku zaoferowania gwarancji dla punktów 1.2.3 OPZ – 48 miesięcy zamawiający przyzna – 20 pkt.
W przypadku zaoferowania gwarancji 60 miesięcy dla punktów 1.2.3 OPZ - zamawiający przyzna- 40 pkt.

Wydłużenie terminy Gwarancji musi dotyczyć punktów 1,2,3 Opisu przedmiotu zamówienia łącznie.
W przypadku nie zaoferowania wydłużonego terminu gwarancji dla któregoś z wymienionych przedmiotów, zamawiający nie przyzna punktów w tym kryterium oferentowi.

Zamawiający nie przyjmuje możliwości zaoferowania terminu gwarancji innego niż podstawowy (36 miesięcy) lub określone powyżej (48 miesięcy lub 60 miesięcy)
W przypadku podania wartości poniżej 36 miesięcy oferta zostanie uznana za nie zgodną z Opisem Przedmiotu zamówienia. W przypadku podania wartości pomiędzy 36 miesięcy a 60 miesięcy a innej niż 48 miesięcy lub 60 miesięcy zamawiający uzna to za okres podstawowy wskazany w OPZ(36 miesięcy) i przyzna 0 pkt.
W przypadku zaoferowania pow. 60 miesięcy zamawiający uzna tą wartość jako 60 miesięcy i przyzna – 40 pkt

2. Liczby punktów w poszczególnych kryteriach **(„CENA”, „DODATKOWY OKRES GWARANCJI”)** zostaną zsumowane. Oferta, która uzyska największą liczbę punktów w poszczególnych kryteriach będzie ofertą najkorzystniejszą. Punktacja będzie liczona z dokładnością do dwóch miejsc po przecinku.

3. Zamawiający udzieli zamówienia wykonawcy, którego oferta odpowiada zasadom określonym w ustawie Prawo zamówień publicznych oraz wszystkim wymaganiom określonym w swz i który uzyskał najwyższą liczbę punktów w wyżej wymienionych kryteriach.

XXI. INFORMACJE O FORMALNOŚCIACH, JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w SWZ i została oceniona jako najkorzystniejsza w oparciu o podane wyżej kryteria oceny ofert.
2. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnieniem art. 577 Pzp, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni, jeżeli zostało przesłane w inny sposób **(art. 308 ust. 2 Pzp).**
3. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 2, jeżeli w postępowaniu o udzielenie zamówienia prowadzonym w trybie podstawowym złożono tylko jedną ofertę **(art. 308 ust. 3 pkt 1 Pzp).**
4. 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.
5. Wykonawca będzie zobowiązany do podpisania umowy w miejscu i terminie wskazanym przez Zamawiającego.
6. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców oraz wybrać ofertę najkorzystniejszą albo unieważnić postępowanie **(art. 263 Pzp).**

XXII. OPIS CZĘŚCI ZAMÓWIENIA

Zamawiający nie dopuszcza możliwość składania ofert częściowych.

XXIII. LICZBA CZĘŚCI ZAMÓWIENIA, NA KTÓRĄ WYKONAWCA MOŻE ZŁOŻYĆ OFERTĘ, LUB MAKSYMALNA LICZBA CZĘŚCI, NA KTÓRE ZAMÓWIENIE MOŻE ZOSTAĆ UDZIELONE TEMU SAMEMU WYKONAWCY, ORAZ KRYTERIA LUB ZASADY, MAJĄCE ZASTOSOWANIE DO USTALENIA, KTÓRE CZĘŚCI ZAMÓWIENIA ZOSTANĄ UDZIELONE JEDNEMU WYKONAWCY, W PRZYPADKU WYBORU JEGO OFERTY W WIĘKSZEJ NIŻ MAKSYMALNA LICZBIE CZĘŚCI

Zamawiający **nie dopuszcza** możliwość składania ofert częściowych.

XXIV. INFORMACJE DOTYCZĄCE OFERT WARIANTOWYCH, W TYM INFORMACJE O SPOSOBIE PRZEDSTAWIANIA OFERT WARIANTOWYCH ORAZ MINIMALNE WARUNKI, JAKIM MUSZĄ OSPOWIADAĆ OFERTY WARIANTOWE

Zamawiający **nie dopuszcza** możliwości składania ofert wariantowych.

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

Zamawiający **nie przewiduje** wymagań w zakresie zatrudnienia na podstawie stosunku pracy, w okolicznościach, o których mowa w art. 95.

XXVI. WYMAGANIA W ZAKRESIE ZATRUDNIENIA OSÓB, O KTÓRYCH MOWA W ART. 96 UST. 2 PKT2

Zamawiający **nie przewiduje** wymagań w zakresie zatrudnienia osób, o których mowa w art. 96 ust. 2 pkt 2.

XXVII. INFORMACJA O ZASTRZEŻENIU MOŻLIWOŚĆI UBIEGANIA SIĘ O UDZIELENIE ZAMÓWIENIA WYŁĄCZNIE PRZEZ WYKONAWCÓW, O KTÓRYCH MOWA W ART. 94

Zamawiający **nie zastrzega** możliwości ubiegania się o udzielenie zamówienia wyłącznie przez Wykonawców, o których mowa w art. 94.

XXVIII. WYMAGANIA DOTYCZĄCE WADIUM, W TYM JEGO KWOTĘ

Zamawiający **nie wymaga** wniesienia wadium.

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

Zamawiający **nie przewiduje** udzielenia zamówienia, o którym mowa w art. 214 ust.1 pkt 7 i 8 ustawy.

XXX. INFORMACJE DOTYCZĄCE PRZEPROWADZENIA PRZEZ WYKONAWCĘ WIZJI LOKALNEJ LUB SPRAWDZENIA PRZEZ NIEGO DOKUMENTÓW NIEZBĘDNYCH DO REALIZACJI ZAMÓWIENIA, O KTÓRYCH MOWA W ART. 131 UST. 2

Zamawiający **nie wymaga** odbycia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia. Wykonawca, przed ustaleniem ceny, może dokonać wizji. Wizji można dokonać po wcześniejszym skontaktowaniu się i umówieniu terminu z Zamawiającym.

XXXI. INFORMACJE DOTYCZĄCE WALUT OBCYCH, W JAKICH MOGĄ BYĆ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ

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

XXXII. INFORMACJE DOTYCZĄCE ZWROTU KOSZTÓW UDZIAŁU W POSTĘPOWANIU

Zamawiający **nie przewiduje** zwrotu kosztów udziału w postępowaniu, z zastrzeżeniem art. 261.

XXXIII. INFORMACJE O OBOWIĄZKU OSOBISTEGO WYKONANIA PRZEZ WYKONAWCĘ KLUCZOWYCH ZADAŃ

Zamawiający **nie zastrzega** obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań.

XXXIV. MAKSYMALNA LICZBA WYKONAWCÓW, Z KTÓRYMI ZAMAWIAJĄCY ZAWRZE UMOWĘ RAMOWĄ

Zamawiający **nie przewiduje** zawarcia umowy ramowej.

XXXV. INFORMACJA O PRZEWIDYWAYM WYBORZE NAJKORZYSTNIEJSZEJ OFERTY Z ZASTOSOWANIEM AUKCJI ELKTRONICZNEJ WRAZ Z INFORMACJAMI, O KTÓRYCH MOWA W ART.230

Zamawiający **nie przewiduje** aukcji elektronicznej.

XXXVI. WYMÓG LUB MOŻLIWOŚĆ ZŁOŻENIA OFERT W POSTACI KATALOGÓW ELEKTRONICZNYCH LUB DOŁĄCZENIA KATALOGÓW ELKTRONICZNYCH DO OFERT

Zamawiający **nie wymaga** złożenia oferty w postaci katalogu elektronicznego

XXXVII. INFORMACJE DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający **nie wymaga** wniesienia zabezpieczenia należytego wykonania umowy.

XXXVIII. POLEGANIE NA ZASOBACH INNYCH PODMIOTÓW

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych
2. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.

3. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów **(art. 118 ust 3 Pzp).** Wzór oświadczenia **stanowi załącznik nr 7 do SWZ.**
4. Zamawiający ocenia, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.
5. Podmiot, który zobowiązał się do udostępnienia zasobów, odpowiada solidarnie z Wykonawcą, który polega na jego sytuacji finansowej lub ekonomicznej, za szkodę poniesioną przez Zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów podmiot ten nie ponosi winy.
6. Jeżeli zdolności techniczne lub zawodowe, sytuacja ekonomiczna lub finansowa podmiotu udostępniającego zasoby nie potwierdzają spełniania przez wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu **(art. 122 Pzp).**
7. **Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby (art. 123 Pzp).**
8. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, **wraz z oświadczeniem, o którym mowa w Rozdziale XVII pkt 1 SWZ, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego**

podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby, zgodnie z katalogiem dokumentów określonych w Rozdziale XVI SWZ (art. 125 ust. 5 PZP).

XXXIX. WYJAŚNIENIA TREŚCI SWZ

1. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ **(art. 284 ust. 1 Pzp).**
   Wszelkie pytania dotyczące wyjaśnienia treści SWZ powinny być wnoszone za pośrednictwem: **https://platformazakupowa.pl/pn/krobia.**
2. Zamawiający jest obowiązany udzielić wyjaśnień **niezwłocznie,** jednak **nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert (art. 284 ust. 2 Pzp).**
3. Jeżeli Zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 2, **przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami** niezbędnymi do należytego przygotowania i złożenia ofert.
4. W przypadkach, o których mowa w ust. 2 i 3 Zamawiający zamieszcza wyjaśnienia za pośrednictwem **https://platformazakupowa.pl/pn/krobia.**
5. Treść zapytań wraz z wyjaśnieniami Zamawiający udostępnia, bez ujawniania źródła zapytania, za pośrednictwem: **https://platformazakupowa.pl/pn/krobia.**
6. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ **(art. 286 Pzp).**
7. Dokonaną zmianę treści SWZ Zamawiający udostępnia za pośrednictwem: **https://platformazakupowa.pl/pn/krobia.**

XL. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Zasady, terminy oraz sposób korzystania ze środków ochrony prawnej szczegółowo regulują przepisy **działu IX ustawy** – Środki ochrony prawnej (**art. 505 – 590 ustawy**)**.**
2. Środki ochrony prawnej przysługują Wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy PZP.
3. Odwołanie przysługuje na:
   1) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania Wykonawców lub konkursie, w tym na projektowane postanowienie umowy;
   2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania Wykonawców lub konkursie, do której Zamawiający był obowiązany na podstawie ustawy;
   3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że Zamawiający był do tego obowiązany
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej.
5. Odwołujący przekazuje Zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
6. Zgodnie z art. 515 ustawy, odwołanie wnosi się:

„1. Odwołanie wnosi się:

1) w przypadku zamówień, których wartość jest równa albo przekracza progi unijne, w terminie:

a) 10 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,

b) 15 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a;

2) w przypadku zamówień, których wartość jest mniejsza niż progi unijne, w terminie:

a) 5 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,

b) 10 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a.

2. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub konkurs lub wobec treści dokumentów zamówienia wnosi się w terminie:

1) 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia dokumentów zamówienia na stronie internetowej, w przypadku zamówień, których wartość jest równa albo przekracza progi unijne;

2) 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej, w przypadku zamówień, których wartość jest mniejsza niż progi unijne.

3. Odwołanie w przypadkach innych niż określone w ust. 1 i 2 wnosi się w terminie:

1) 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia, w przypadku zamówień, których wartość jest równa albo przekracza progi unijne;

2) 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia, w przypadku zamówień, których wartość jest mniejsza niż progi unijne.

4. Jeżeli Zamawiający nie opublikował ogłoszenia o zamiarze zawarcia umowy lub mimo takiego obowiązku nie przesłał Wykonawcy zawiadomienia o wyborze najkorzystniejszej oferty lub nie zaprosił Wykonawcy do złożenia oferty w ramach

dynamicznego systemu zakupów lub umowy ramowej, odwołanie wnosi się nie później niż w terminie:

1) 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo 30 dni od dnia publikacji w Dzienniku Urzędowym Unii Europejskiej ogłoszenia o udzieleniu zamówienia, a w przypadku udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki – ogłoszenia o wyniku postępowania albo ogłoszenia o udzieleniu zamówienia, zawierającego uzasadnienie udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki;

2) 6 miesięcy od dnia zawarcia umowy, jeżeli zamawiający:

a) nie opublikował w Dzienniku Urzędowym Unii Europejskiej ogłoszenia o udzieleniu zamówienia albo

b) opublikował w Dzienniku Urzędowym Unii Europejskiej ogłoszenie o udzieleniu zamówienia, które nie zawiera uzasadnienia udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki;

3) miesiąca od dnia zawarcia umowy, jeżeli Zamawiający:

a) nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo

b) zamieścił w Biuletynie Zamówień Publicznych ogłoszenie o wyniku postępowania, które nie zawiera uzasadnienia udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki.”

7. Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie – sądu zamówień publicznych, zwanego „sądem zamówień publicznych”.
8. Skargę wnosi się za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1, przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe jest równoznaczne z jej wniesieniem.

9. Od wyroku sądu lub postanowienia kończącego postępowanie w sprawie przysługuje skarga kasacyjna do Sądu Najwyższego.

XLI. OCHRONA DANYCH OSOBOWYCH

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

- wykonawcy będącego osobą fizyczną;
- wykonawcy będącego osobą fizyczną, prowadzącą jednoosobową działalność gospodarczą;
- pełnomocnika wykonawcy będącego osobą fizyczną (np. dane osobowe zamieszczone w pełnomocnictwie);
- członka organu zarządzającego wykonawcy, będącego osobą fizyczną (np. dane osobowe zamieszczone w informacji z KRK);
- osoby fizycznej skierowanej do realizacji, przygotowania i przeprowadzenia postępowania o udzielenie zamówienia publicznego lub do kontaktów w sprawie realizacji zamówienia.

Zamawiający informuje:

- Administratorem Państwa danych osobowych Urząd Miejski w Krobi, ul. Rynek 1, 63-840 Krobia listownie na adres: Urząd Miejski w Krobi, ul. Rynek 1, 63-840 Krobia;
- poprzez e-mail: krobia@krobia.pl;
- telefonicznie: +655 711 111.

1. **Inspektor ochrony danych**

   W sprawach związanych z Pani/Pana danymi proszę kontaktować się z Inspektorem Ochrony Danych, kontakt pisemny za pomocą poczty tradycyjnej na adres: UM w Krobi, za pomocą poczty elektronicznej na adres e-mail: iod@krobia.pl

2. **Cel przetwarzania**

   Państwa dane osobowe przetwarzane będą w celu:

- **prowadzenia postępowania o udzielenie zamówienia publicznego,** którego podstawą są warunki zamówienia ustalone przez administratora, prowadzącego do wyboru najkorzystniejszej oferty lub wynegocjowania postanowień umowy w sprawie zamówienia publicznego, kończące się zawarciem umowy w sprawie zamówienia publicznego albo jego unieważnieniem (na podstawie art. 6 ust. 1 lit. b i lit. c RODO),
- **rozpoznania rynku** w przypadku zamówienia z wolnej ręki lub w przypadkach realizacji zamówień o wartości mniejszej niż ustawowy próg od którego stosuje się przepisy dotyczące zamówień publicznych (na podstawie art. 6 ust. 1 lit. f RODO);

zgodnie z wymaganiami określonymi w:

- ustawie z dnia z dnia 11 września 2019 r. Prawo zamówień publicznych [PZP];
- rozporządzeniu 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;
- ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

3. Odbiorcy danych osobowych

- Państwa dane pozyskane w związku z postępowaniem o udzielenie zamówienia publicznego przekazywane będą wszystkim zainteresowanym podmiotom i osobom, gdyż co do zasady postępowanie o udzielenie zamówienia publicznego jest jawne.
- Ponadto odbiorcą danych zawartych w dokumentach związanych z postępowaniem o zamówienie publiczne mogą być podmioty z którymi Administrator zawarł umowy lub porozumienia na korzystanie z udostępnianych przez nie systemów informatycznych w zakresie przekazywania lub archiwizacji danych. Zakres przekazania danych tym odbiorcom ograniczony jest jednak wyłącznie do możliwości zapoznania się z tymi danymi w związku ze świadczeniem usług wsparcia technicznego i usuwaniem awarii. Odbiorców tych obowiązuje klauzula

zachowania poufności pozyskanych w takich okolicznościach wszelkich danych, w tym danych osobowych.

4. **Okres przechowywania danych**

   Dane osobowe zebrane w związku z postępowaniem o udzielenie zamówienia publicznego będą przetwarzane przez okres 4 lat - dla dokumentów wytworzonych w ramach zamówień publicznych krajowych, lub 10 lat - dla zamówień publicznych unijnych - licząc od 1 stycznia roku następnego od daty zakończenia sprawy.

5. **Przekazywanie danych poza Europejski Obszar Gospodarczy**

   W związku z jawnością postępowania o udzielenie zamówienia publicznego Państwa dane mogą być przekazywane do państw z poza EOG. Ograniczenie dostępu do Państwa danych może wystąpić jedynie w szczególnych przypadkach, jeśli jest to uzasadnione ochroną prywatności zgodnie z art. 18 ust. 5 i 6 oraz z art. 74 ust. 4 ustawy PZP.

6. **Uprawnienia związane z przetwarzaniem danych osobowych**

   Posiada Pan/Pani:

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

- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

nie przysługuje Pani/Panu:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO; na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

7. Obowiązek podania danych

Podanie danych osobowych w związku z udziałem w postępowaniu o zamówienia publiczne nie jest obowiązkowe, ale może być warunkiem niezbędnym do wzięcia w nim udziału. Wynika to stąd, że w zależności od przedmiotu zamówienia, zamawiający może żądać ich podania na podstawie przepisów ustawy PZP zamówień publicznych oraz wydanych do niej przepisów wykonawczych, a w szczególności na podstawie 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. Konsekwencje niepodania określonych danych wynikają z w/w ustawy.
Jednocześnie Zamawiający przypomina o ciążącym na Pani/Panu obowiązku informacyjnym wynikającym z 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, chyba że ma zastosowanie co najmniej jedno z wyłączeń, o których mowa w art. 14 ust. 5 RODO.

XLII. SPIS ZAŁĄCZNIKÓW

1. Formularz ofertowy – **załącznik nr 1**

2. Oświadczenie o spełnianiu warunków udziału w postępowaniu – **załącznik nr 2**
3. Oświadczenie o niepodleganiu wykluczeniu w postępowaniu **– załącznik nr 3**
4. Wykaz dostaw - **załącznik nr 5**
5. Oświadczenie Wykonawców wspólnie ubiegających się o zamówienie – **załącznik nr 6**
6. Zobowiązanie podmiotu udostępniającego zasoby – **załącznik nr 7**
7. Wzór umowy – **załącznik nr 8**